APPLICATION OF DIGITAL TECHNIQUES TO A NUCLEAR REACTOR SAFETY MONITOR FOR THE LIQUID METAL FAST BREEDER REACTOR

Stephen Anthony Elrod

NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

APPLICATION OF DIGITAL TECHNIQUES
TO A NUCLEAR REACTOR SAFETY MONITOR
FOR THE LIQUID METAL FAST
BREEDER REACTOR

by

Stephen Anthony Elrod

Thesis Advisor: M. L. Cotton

March 1972

Application of Digital Techniques to a Nuclear
Reactor Safety Monitor for the
Liquid Metal Fast Breeder Reactor

by

Stephen Anthony Elrod
Lieutenant Commander, United States Navy
B.E.E., Auburn University, 1962

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN ELECTRICAL ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
March 1972

ABSTRACT

This paper demonstrates a nuclear reactor safety monitor incorporating hard-wired, redundant, digital program modules that control independent, redundant, digital monitor modules. One monitor module is used for each parameter significant to reactor safety. The characteristics of a proposed LIQUID METAL FAST BREEDER REACTOR are used as the reference performance criteria. The established criterion that a single failure must not prevent reactor shut down is used as the failure mode criterion. Within the program module, a programmable read-only memory (PROM) is used for sequence control of another PROM containing variable length subroutines. The subroutine PROM outputs are used as photo-isolated logic outputs for sequence control of the various monitor modules. The program module action is modelled on a digital computer. A four-input digital monitor module is developed. This module provides a shut down signal if three of the inputs exceed the parameter limit.

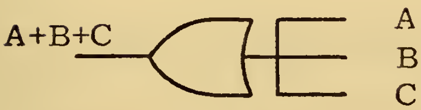
TABLE OF CONTENTS

LIST OF TABLES

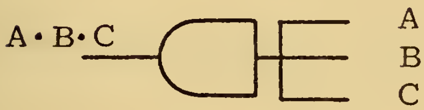
LIST OF FIGURES

Table I. TABLE OF SYMBOLS

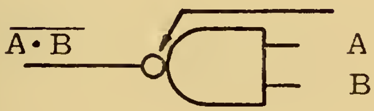
An Event or Result



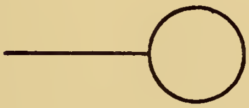
Logical "OR" - Output occurs if any of the inputs occur.



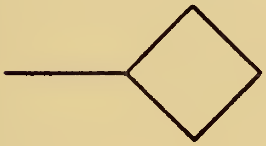
Logical "AND" - Output occurs only if all the inputs occur.



Logical "NOT" - Output of function is inverted.



Basic Fault-The fault requires no further analysis.



Fault Basic to a Given Tree-The fault can be caused by even more basic failures.

Transfer In-Preceeding events occur elsewhere on the fault tree.

Transfer Out-The result of this event also effects another section of the fault tree.

ACKNOWLEDGMENTS

The author acknowledges his gratitude to his wife for the days of typing and re-typing of drafts of this work. Her willingness to do this during preparations for moving certainly deserves commendation.

Also, to Professor M. L. Cotton of the Naval Postgraduate School, who helped the author greatly with his suggestions and encouragement.

I. INTRODUCTION

The rapidly increasing electrical power demands in the United States and the resultant decreasing availability of natural fuels has caused a great demand by utility companies for nuclear powered generating stations of any kind. This, in turn, has placed heavy demands on the nation's ability to process from natural ores the amounts of fissile (i.e., easily split by neutron interaction into by-products and excess high-energy neutrons) uranium and plutonium required to fuel the reactors. These are mostly light-water moderated, thermal reactors which operate at moderate temperatures (500-700 F) and use saturated steam to power the electric generators. Much larger but presently little used supplies of uranium, thorium, and plutonium are not easily fissionable in their natural state but do easily absorb neutrons and become fissile materials suitable for reactor fuels. These materials are referred to as "fertile."

During the 1960's a development program was instituted by the United States Atomic Energy Commission (AEC) to develop sodium cooled fast breeder reactor plants intended to convert fertile fuel into fissile fuel (breeding) in addition to supplying electricity. Since coolant temperatures are higher in this process, more efficient conversion of thermal energy into electrical energy is feasible also. The potential result is enhanced availability of nuclear fuel, both by breeding

and by increased plant efficiency. (See Appendix A, the introduction to the LIQUID METAL FAST BREEDER REACTOR (LMFBR) DEVELOPMENT PLAN, v. 1. [Ref. 1]).

The LMFBR Development Plan [Ref. 1] presents the state-of-the-art advances required by the much harsher environment characterized by higher neutron and gamma fluxes, higher temperatures, and liquid metal coolant. These documents indicate that current levels of technology are unsatisfactory in almost all areas and that concurrent research is being pursued. References 6-9 indicate some of this research with respect to reactor instrumentation. Reference 6 discussus the test facilities required and efforts to upgrade test environments from 700 F to 1400 F, 10^9 nv thermal-neutron flux to 10^{16} nv fast-neutron flux, and 10^4 R/h to 10^9 R/h gamma flux. Research efforts in sensor development for temperature (thermocouples), neutron flux, flow, pressure, level, and strain are also discussed. Reference 7 discussus a possible microwave temperature sensor configuration. Reference 8 reports work on in-core, self-powered, fast-neutron flux monitors. Reference 9 discussus the problems of radiation induced noise on electrical signal cables. The varying approaches taken by the researchers indicate that optimum instrumentation techniques are yet to be proven.

The exact configuration of the reactors and controls, and the methods of detecting, transmitting, and utilizing various parameters are undetermined. This situation forces the use of assumptions of

most likely future conditions. Published feasibility studies have provided insight into probable reactor designs and those parameters required to be measured and used for safety considerations. Reference 10, a good example of such a study based on the estimated state of the technology in 1980, proposes a 3-loop, double heat exchange, 1150 F, 2415 Mwt, 43% efficient plant, with a fuel doubling time of 14.3 years, and a core lifetime of 605 full power days. Direct digital control is proposed for many operations in the plant, including safety system backup. Figure one illustrates the referenced concept of the plant control system, primarily analog. The importance of the figure to this work is its use as an illustration of typical relationships among control parameters. Figure two shows the referenced plant's gross relationship between the control systems of figure one and the digital computer. The analog safety monitor system operates as part of the "Nuclear Safety and Control System" to provide safety actions if parameter limits are exceeded. An important point not clear in the figure is the required independence of the nuclear safety and nuclear control systems. Functions which initiate safety shutdown are:

1. high outlet temperature
2. high start up rate
3. high power level
4. low flow rate
5. low coolant level
6. high neutron flux/flow rate
7. turbine generator trip

8. loss of feedwater

9. loss of heat sink

10. loss of vital instrument power

11. manual trip

Reference 10 is not a final study and does not develop the hardware to accomplish the objectives.

The safety criteria discussed in the various publications are all based on the concept of preventing a power excursion or other event that could damage the core and release activity to the coolant or atmosphere. From this concept, several criteria pertinent to this investigation have been developed:

1. The nuclear power plant protection system shall, with precision and reliability, automatically initiate appropriate protective action whenever a plant condition monitored by the system reaches a pre-set level.

2. Components and modules shall be of a quality that is consistent with minimum maintenance requirements and low failure rates.

3. Channels that provide signals for the same plant protective function shall be independent and physically separated.

4. Any single equipment failure within the protective system shall not prevent proper protection system action when required (single failure criterion).

These criteria have resulted in multiple safety channels, multiple power supplies, and required periodic testing of safety channels. References 11-15 discuss many of these concepts in detail. In any case, each individual reactor installation must be reviewed and approved by the AEC prior to operation.

Presently, analog safety systems provide the proper isolation and redundancy for a safety system but suffer from additive errors due to the series arrangement of components; widening the margin between an allowed indicated condition and allowed actual condition. Since multiple adjustments are provided in analog channels, they must be regularly checked to ensure that they are still within allowed tolerances. A digital form of data transmission appears to be capable of providing channel separation, and yet can both reduce the number of error introducing components in the safety circuit and be made largely self-checking.

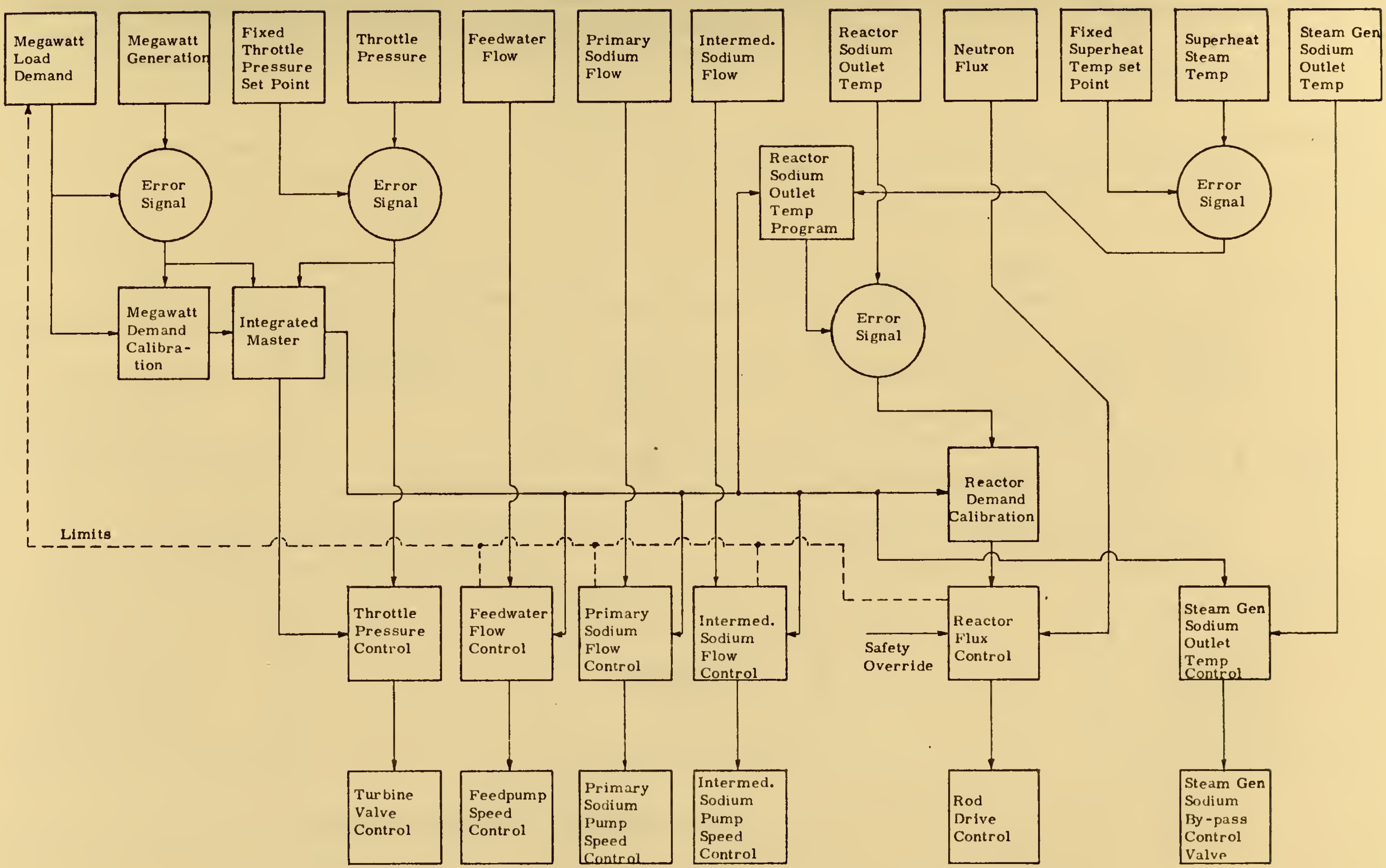
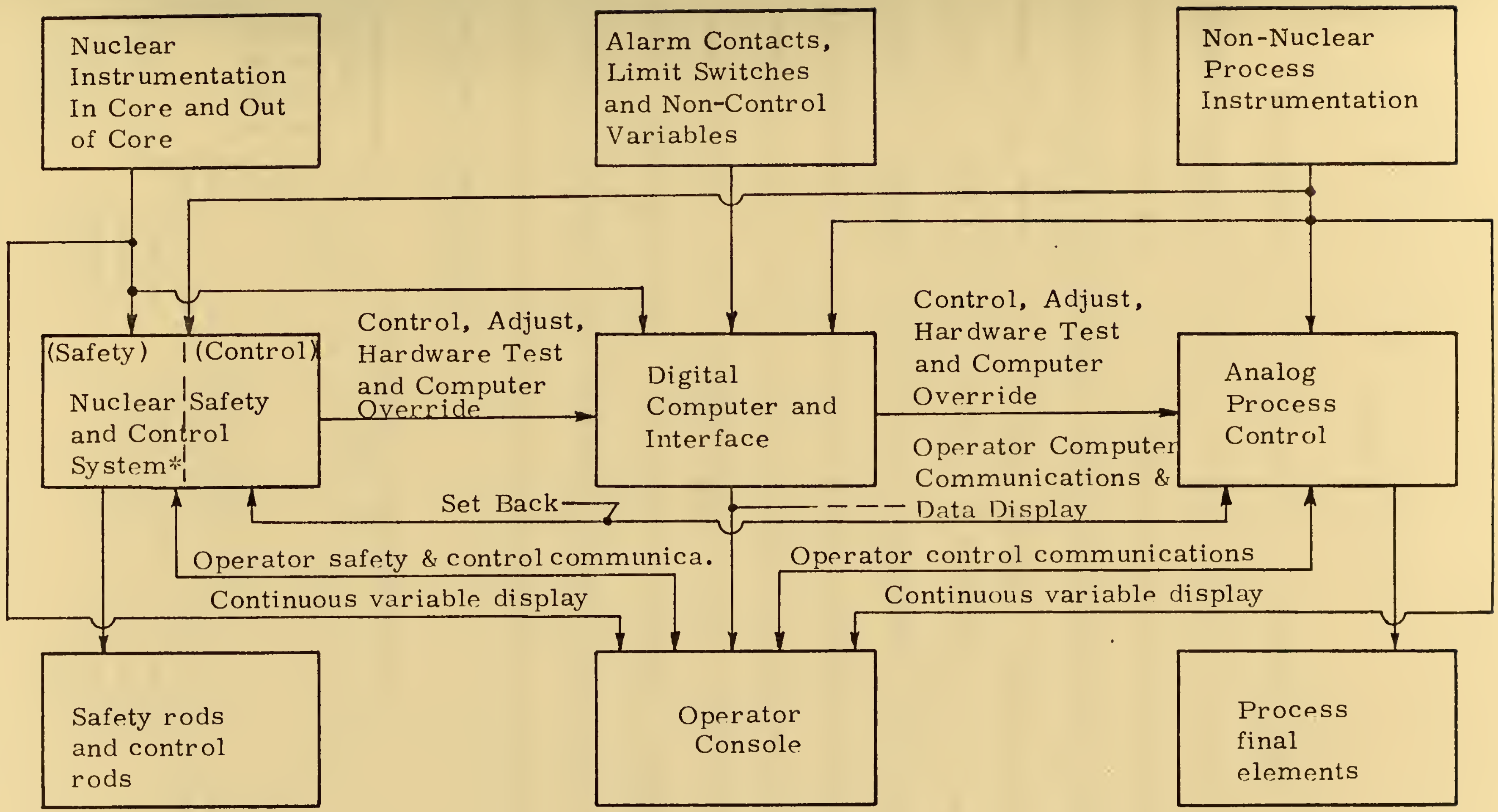


Figure 1. LMFBR CONTROL SYSTEM [Ref. 10]



*Note: Separation of safety and control functions required.

Figure 2. LMFBR SYSTEMS AND INSTRUMENTATION COMMUNICATIONS CHANNELS [Ref. 10]

II. OBJECTIVES

Consideration of current practice in reactor control design, digital techniques, and safety criteria, coupled with anticipated requirements [Refs. 1-5, 10, Appendix B], led to the conclusion that some digital technique should provide a reliable and acceptable safety monitoring system for the LMFBR. Figure 3 illustrates the overall approach taken by this investigator in developing such a safety monitor system. Two basic concepts were incorporated. One concept was to have each safety parameter channel and its monitor module independent of the others and to have each channel comply with the conditions required in Sec. II B, ASSUMPTIONS, and Sec. II C, CRITERIA FOR IDEAL PERFORMANCE, of this report. The other concept was to provide a redundant and independent program module that would control the operation of the various monitor modules yet maintain their individual independence.

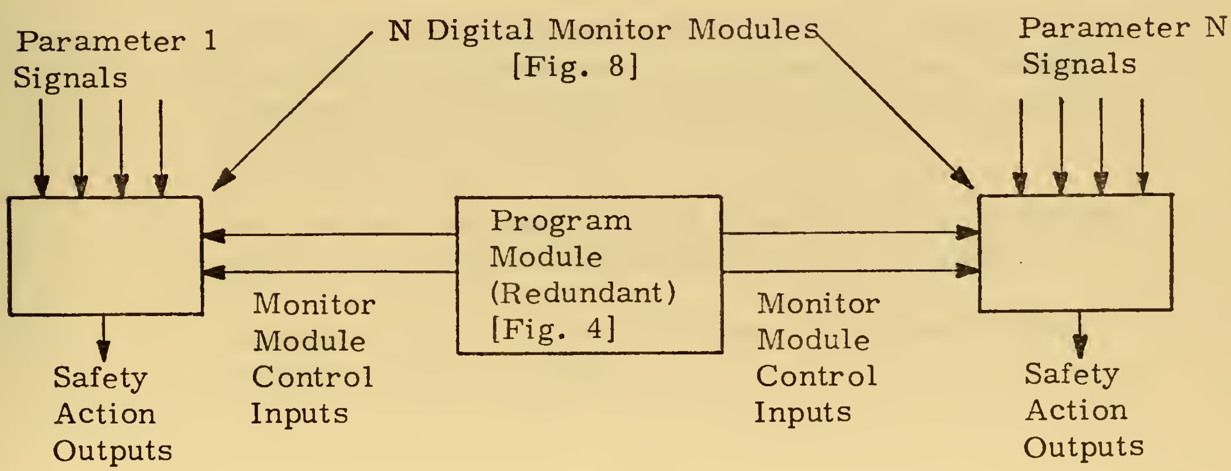


Figure 3. OVERALL APPROACH TO A DIGITAL SAFETY MONITOR

A. OBJECTIVES OF THIS INVESTIGATION

The objective of this investigation was to provide the following within the framework of LMFBR operation:

1. Compare the characteristics of sequential-step stored-program design with sequential-step hard-wired design of a monitor within the framework of speed, program hardness, and separability of channels.

2. Design a solid-state program module that would replace a stored program, maximize parallel-parameter operation of the safety monitor, and provide for field program changes.

3. Determine how closely this solid-state program module satisfied the ideal monitor criteria.

4. Demonstrate, by designing a digital monitor module, a digital method of monitoring one safety parameter. Investigate the extent to which safety channel separability, self test, and abnormal operation determination could be maintained in this one parameter channel.

B. ASSUMPTIONS

Since the LMFBR was undeveloped, assumptions were required to provide a framework for investigation:

1. The LMFBR configuration of Ref. 10 was to be used. Pertinent details of the configuration are listed in the introduction.

2. On-line digital computer control would be used. References 16-23 support this contention and discuss sampled-data techniques, optimal control, and several presently-installed digital control systems.

3. The control computer, though separate from the safety system, would have the safety limits programmed.

4. The environmental and performance requirements of Appendix B must be met.

5. A separate monitor unit for safety parameters would be used in addition to the on-line control computer to provide two independent mechanisms for actuating the safety shut down system.

C. CRITERIA FOR IDEAL PERFORMANCE

Ideally this monitor should satisfy the following criteria:

1. Operate with sufficient speed to protect the LMFBR. Reference 10 mentions a minimum delay of 100 msec. with 200 msec. more probable.

2. Maintain reactor protection if control computer fails.

3. Monitor failure should not prevent the control computer from initiating reactor shutdown.

4. Be compatible with control computer operation.

5. Have a program that:

    a. Is hard under all operational conditions.

    b. Can be changed without disturbance of wiring.

6. Be more reliable than the control computer.

7. Detect its own abnormal operation.

8. Operate without large storage requirements or need for external devices such as tapes.

9. Provide a means to change safety limits easily for plant maintenance.

10. Be modularized to minimize downtime.

III. COMPARISON OF SMALL SEQUENTIAL-STEP STORED-PROGRAM AND HARD-WIRED COMPUTERS

The general public acceptance of minicomputers for dedicated control and monitoring applications prompted an investigation of the utility of these machines with respect to LMFBR safety monitor implementation. The literature describing these machines emphasizes reliability, low cost, expandable configuration, and custom-tailored functions. All of these assets would be pertinent to LMFBR utilization provided that speed, channel separation, and single failure criteria were met.

A. IMPORTANT CHARACTERISTICS OF SMALL SEQUENTIAL STEP STORED-PROGRAM COMPUTER

A small sequential-step stored-program computer (minicomputer) stores its program and data in core memory and executes the program step by step at the register transfer level. Though some may use a read-only memory to control the arithmetic unit and registers, allowing several arithmetic operations or register transfers (some simultaneously) per core memory cycle time, the program steps are executed sequentially at the operation level; i.e., multiply, divide. The storing of the basic operations in a read-only memory is sometimes called "firm-wired." Typical cycle time is 1-2 microseconds for each simple operation (one read-write time).

The most important characteristic features that restrict the utility of these machines for the nuclear monitoring application are:

1. Storage in the computer memory unit of both program sequence and data. Inherently, the program and the data from the various safety channels in a reactor safety monitor environment are brought together, violating the philosophy of monitor channel separation.

2. Common busses for data transfer. Again, one failure can effect both program and data if the bus is associated with the memory unit. One failure can effect data from all safety channels if the failure is associated with a data bus.

3. Sequential data handling. In a small machine, no provision is made for parallel handling of data from more than one source at a time.

4. Requirements for external equipment to input the program if it fails or if safety limits require changing.

5. Checkout programs cannot be independently run in parallel with the main program.

B. IMPORTANT CHARACTERISTICS OF SMALL SEQUENTIAL-STEP HARD-WIRED COMPUTERS

A small sequential-step hard-wired computer maintains its main program in its wiring or read-only memory thus eliminating a stored program.

Important characteristic features:

1. Can operate at faster speeds because a read-write cycle into core memory is not required to access the program.

2. Retains sequential steps for the main program.

3. Simple machines tend to retain common data busses and a single arithmetic unit.

4. Expansion to provide parallel data handling appears to be easier to accomplish than with a primarily software machine.

5. The wiring or hard memory must be changed to change the program sequence.

6. Application of the single failure criterion requires multiple hardware.

7. Test programs either result in interbus connections, destroying channel separation, or must be externally applied.

C. COMPARISON AND CONCLUSION

Comparison of the characteristics of stored-program design with hard-wired design led to the conclusion that a small stored-program device was unsatisfactory and to the search for a device that would utilize the desirable features, such as higher speed and a hard program, of a hard-wired computer, improve the ability to provide for simultaneous parallel operation of independent steps, incorporate self-test while providing data channel isolation, and reduce the amount of hardware needed to provide redundancy. The result was the Program Module described in this paper.

IV. PROGRAM MODULE DESIGN

A. GENERAL CONSIDERATIONS

The first tasks encountered in the design of the program module were the selection of suitable memory and micrologic systems. Particular emphasis was placed on availability and variety of packaged functions, compatability between memory and micrologic, speed of operation, temperature range allowed, and resistance to propagation of failures. A field-programmable, read-only memory (PROM) concept was selected because it offered a hard, but easily changeable, program in an integrated form. Transistor-transistor logic (TTL) medium scale integration (MSI) logic gates and setable counters (Registers) were selected because they appeared to provide a wider range of packaged complex functions and higher speed than the metal-oxide-semiconductor (MOS) type logic. Other attributes of TTL are: a wide range of allowed operating temperature (-55C to +125C), input diode clamping to reduce line-noise reflections, and a wide variety of speed and power specifications.

The program module for the monitor [Fig. 4] was based on the concept that some parameters must be monitored at shorter periods than others, such that the longer monitor periods could be made some multiple of the shortest one. This allowed a simple synchronization scheme with longer-period events inserted at the appropriate time.

Appendix B supports this concept. It was possible then to make each monitor event or test sequence a subroutine that could be called at the proper time. Two clock frequences were required; one at the subroutine operating frequency and one to synchronize the shortest monitor period. The output of the subroutine PROM consisted of dedicated bits, confining the effect of a bit failure compared to the effect if decoders were to be used in conjunction with the PROM output. The dedicated bit concept allows the system designer a great deal of latitude in the use of parallel and concurrent monitor events and in the use of feedback within the control module to control subroutines of varying lengths.

The problem of electrical and physical isolation was solved by application of photo-isolators to the subroutine PROM outputs. A photo-isolator is a packaged unit consisting of a light-emitting diode, a photo-sensitive transistor or reverse-biased diode, and a clear insulator between them. The only connection between the input and output is light.

The output of the diode-transistor type photo-isolator is compatable with TTL inputs but the signal rise and fall times are much too long (5-20 microseconds) to be useful in this application. The output of the diode-diode type photo-isolator is not directly compatable with TTL inputs. A MOS input-TTL output buffer has been developed that operates at TTL voltage and reduces propagation delay to the .05-.1 microsecond range. This device allows the use of the diode-diode photo-isolator configuration.

B. DESCRIPTION OF A PROGRAM MODULE [Fig. 4]

1. Subroutine PROM (RS)

The subroutine PROM (RS) is a 1024 word x (N+2) bit PROM where N is based on overall monitor requirements. With the exception of the two feedback control bits, the output of RS is arbitrary and each bit is dedicated to some function to be performed. Feedback bus RSA holds a logical "1" only when that word is the last word of a subroutine, and feedback bus RSB holds a logical "1" only when that word is the first word of a subroutine. A subroutine may be of arbitrary length but must be at least two words long. Propagation times in the feedback paths also require that, at the 10 MHZ clock frequency, each subroutine be at least two words long. The longest propagation time is in the PROM itself and is limiting; considering that faster counters and logic gates exist.

2. Subroutine Address Register (SAR)

The subroutine address register is a ten bit binary counter. During a subroutine the counter counts up one count each clock pulse; incrementing the address of RS by one. At the end of a subroutine, logic into the CET and $\overline{PE}$ (active low, parallel enable) inputs causes incrementing to stop and, when conditions pre-determined by logic on bus RPB are met, the first address in the next subroutine to be entered by parallel input from the program PROM-RP. Since only eight parallel input lines are available in the basic configuration, the number of preset addresses is only one fourth of the total number of addresses in

SAR and RS. Two hundred fifty six separate subroutines seem to be adequate, considering that PROM dedicated bits may be used regardless of the subroutine involved, but, if more subroutines were required, the PROMs and registers could be expanded.

3. Program PROM (RP)

The sequence of subroutines is stored in PROM-RP (256 words by 12 bits) and sequentially executed. An eight bit bus, RPC, contains the start address of the next subroutine, a three bit bus, RPA, contains the number of times the next subroutine is to be repeated prior to going on, and a one bit bus, RPB, contains a logical "0" if the start of the next subroutine must be synchronized with the sync input. Since the main program and the subroutines are contained in different PROMs, they can be changed independently.

4. Program Count Register (PCR)

The program count register [Fig. 6] is a four bit binary up/down counter that counts down, being clocked by bits on bus RSB; therefore, one count occurs per subroutine. When 0000 is reached the terminal-count-low or borrow gate enables the program address register PAR. At the start of the next subroutine, PAR is incremented and PCR goes to 1111 (binary). After the first step of the subroutine, PCR receives parallel inputs for the number of repeats of the next subroutine.

5. Program Address Register (PAR)

The program address register is an eight bit binary counter similar to SAR. It is enabled by the PCR terminal-count-low gate and uses the RSB output as a clock.

6. Enable Logic for the Subroutine Address Register (SAR)

$(\overline{PE}) = (RSA \cdot (RPB + SYNC))$ - i.e., parallel entry is permitted only at the end of a subroutine and, if required by RPB = "0," at a sync pulse.

$(CET) = (SYNC + RPB + \overline{RSA})$ - i.e., both counting up and parallel entry are inhibited at the end of a subroutine unless conditions for $\overline{PE}$ are met. These gates are constructed as shown in Fig. 5 and consist of one standard MSI chip each.

7. Reset Circuitry

The reset circuitry consists of two elements. Upon initial turn-on or recovery of voltage, one element (low-voltage reset) resets the PAR, resets the SAR, and enables the parallel input into the PCR. Upon encountering a 111 (binary) on bus RPA (end of programmed portion of program PROM), the second element (end-of-program reset) resets the PAR only. The low-voltage reset may consist of a delay device to hold the resets and parallel enable low until after Vcc has risen. The end-of-program reset consists of a simple three-input NAND gate.

C. FAULT TREE OF A PROGRAM MODULE

Table I shows the symbols used in constructing all fault trees in this paper. Figure 7 is the fault tree of the control module.

1. Power Supply Failures

Power supply failures were not included in the control module fault tree because a loss of voltage would cause the control module to reset and a catastrophically high voltage would cause burn-out of the light-emitting diodes in the photo-isolators, having the same effect as a reset. Provision is made in the digital monitor module construction for voting inputs from three parallel program modules; thus preventing a single failure of a program module from inhibiting monitor operation.

2. Analysis with Respect to the Single Failure Criterion

Review of the fault tree of the program module revealed that, while the module contains several feedback paths, the effect of any fault is to prevent proper output; hence a serial fault tree and implied serial consideration of reliability. The serial nature of faults dictates redundant program modules to satisfy the single failure criterion [Ref. 14] which states that no single failure may prevent reactor shut down.

D. TEST REQUIREMENTS FOR THE PROGRAM MODULE

Self-test circuitry in the program module cannot test the connecting wiring between the program module and monitor modules and performs little function not tested elsewhere. It also tends to reduce both

the dedication of PROM-RS dedicated bits and the reliability, due to increased complexity, of feedback paths. It was decided, based on these deleterious conditions, coupled with the simple implementation of redundant program modules, to provide for testing at the monitor module level.

E. COMPUTER MODEL OF THE PROGRAM MODULE

Operation of the program module was tested using a digital computer model [Appendix C]. The functional requirements for the reset circuitry were developed using this model. The model verified that the program module configuration of Fig. 4 operated in the desired manner.

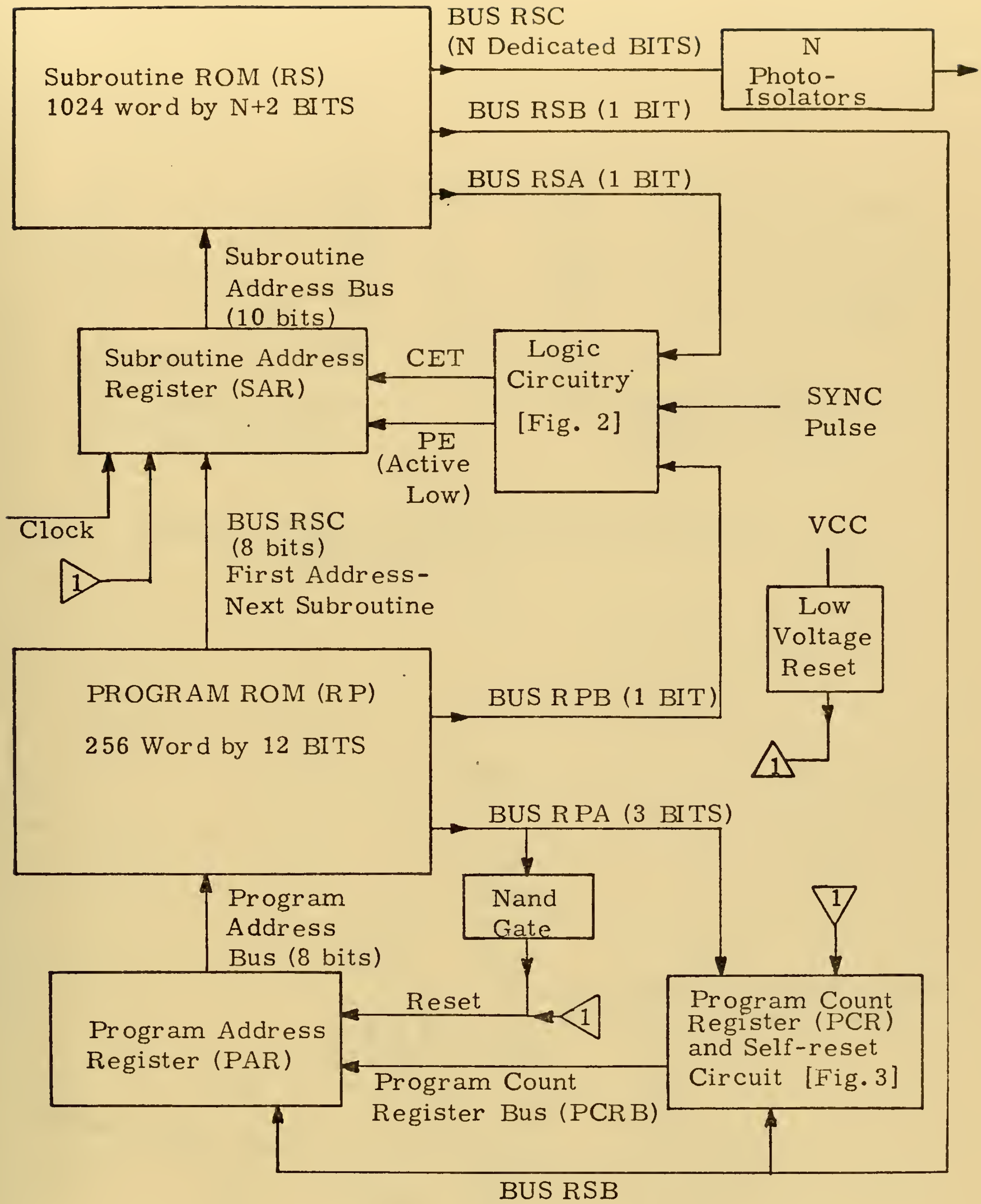
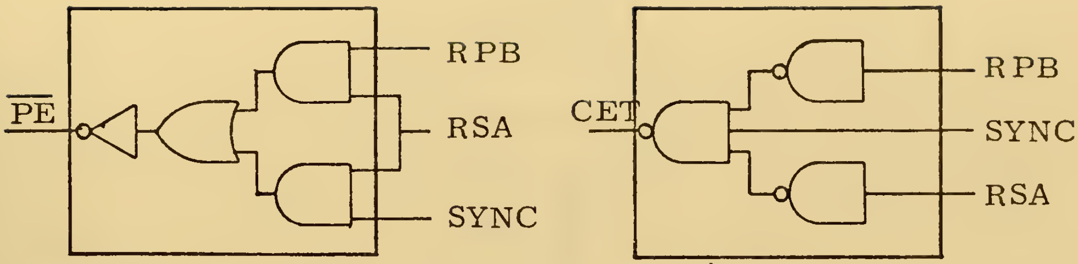


Figure 4. PROGRAM MODULE BLOCK DIAGRAM



A. $\overline{PE}$ input logic
and-or-not IC

B. CET input logic
multiple nand IC

Figure 5. SUBROUTINE ADDRESS REGISTER LOGIC GATES

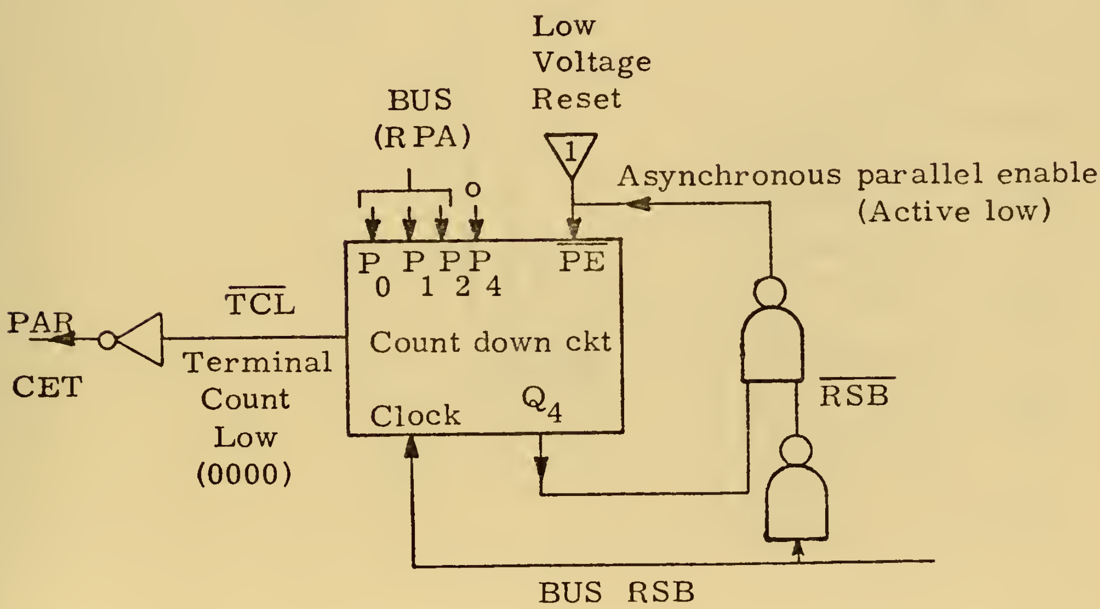
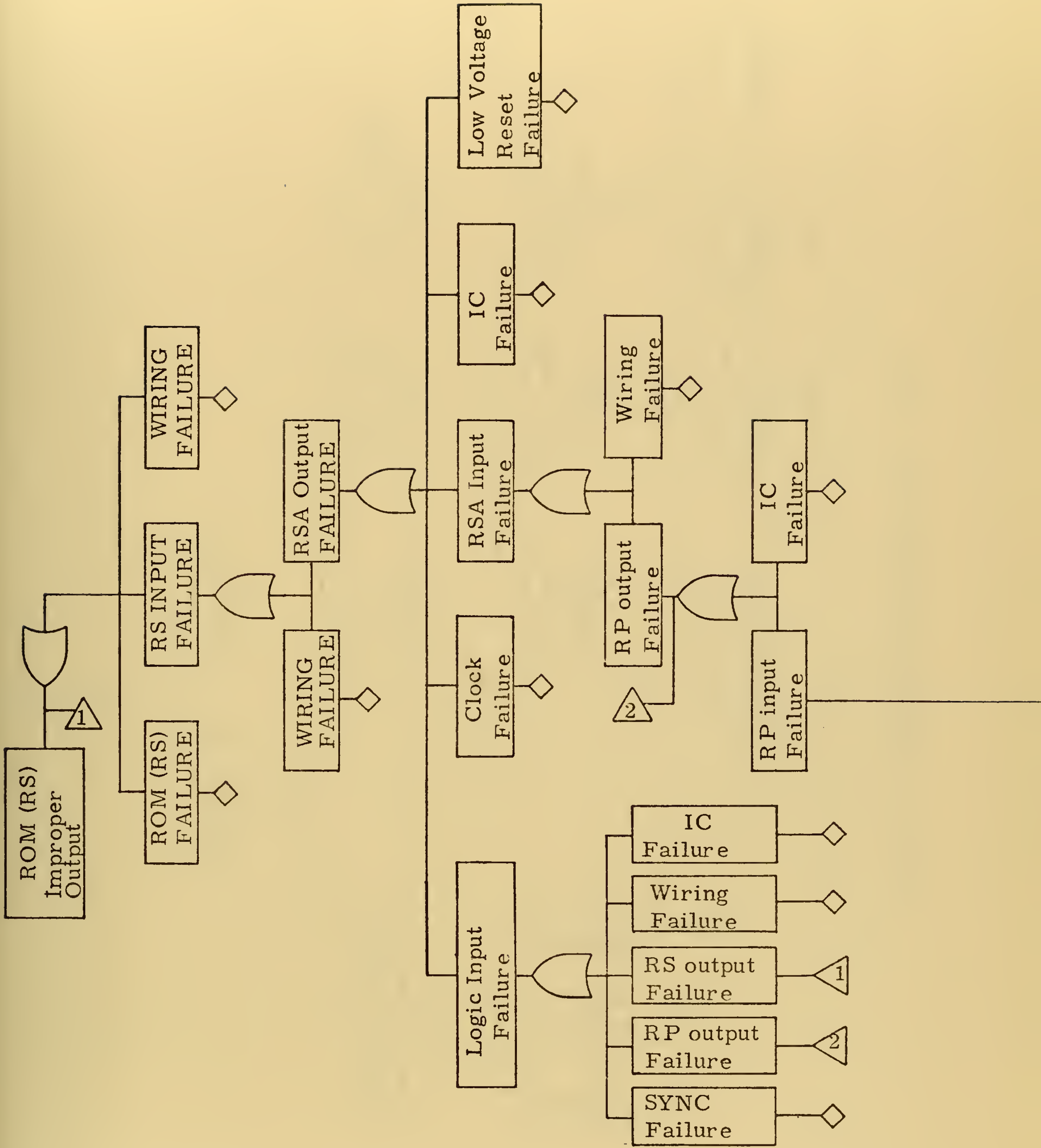


Figure 6. PROGRAM COUNT REGISTER


ROM (RS) Improper Output
ROM (RS) FAILURE
RS INPUT FAILURE
WIRING FAILURE
WIRING FAILURE
RSA Output FAILURE
RSA Input Failure
Low Voltage Reset Failure
IC Failure
Clock Failure
Logic Input Failure
Wiring Failure
RP output Failure
IC Failure
RP input Failure
IC Failure
Wiring Failure
RS output Failure
RP output Failure
SYNC Failure
1
2

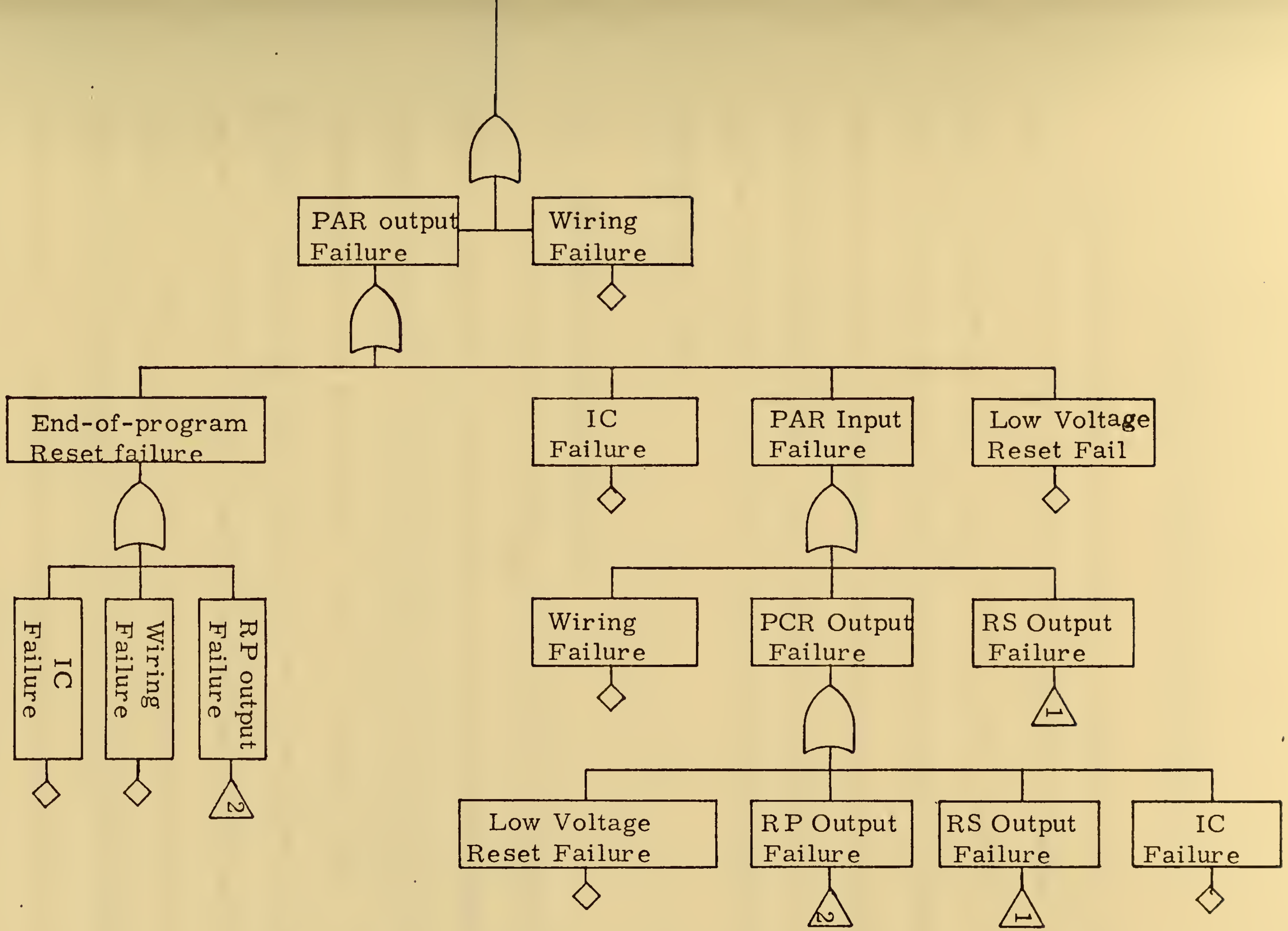


Figure 7. PROGRAM MODULE FAULT TREE

V. DIGITAL MONITOR MODULE DESIGN

This section describes the design of a Digital Monitor Module whose function is, under the control of the program module, to compare four independent digital signals representing a safety parameter with a digital representation of the parameter limit and provide two independent shut down signals if three of the four incoming signals exceed the parameter limit. The module test facilities provide for functional test of the module and, coupled with other monitor modules, the program modules.

A. GENERAL CONSIDERATIONS

In a four-parameter channel, the detectors are usually grouped into two sub-groups for power source and signal channel considerations as shown in Figure 8. Each sub-group is powered from at least two independent sources determined by the overall plant design. Detectors A and C would be associated with power bus I and signal channel I, and detectors B and D would be associated with power bus II and a signal channel II. Reference 14 requires that Channel I and associated circuitry must be physically and electrically isolated from channel II and its circuitry, yet at some point the signals must be combined to provide two independent safety shut down (SCRAM) channels, each representing a combination of data from all four sources. The inability to provide electrical isolation using integrated circuits severely limits the use of

such circuits in the logic design of such a channel. The module design effectively copes with that limitation.

The portion of interest of Figure 8 is inside the dotted lines, and consists of the comparater modules and scram logic modules. These modules, while independent, are controlled by redundant program modules.

B. SPECIFIC DESIGN CHARACTERISTICS EMPLOYED

1. Comply with the philosophy of separation of scram channels.
2. Incorporate integrated circuits to the extent that the failure of one IC does not interrupt both safety signals in a signal channel.
3. Indicate an unsafe reactor condition upon loss of power to the module or component that processes a signal.
4. Prevent the propagation of device failure throughout the monitor.
5. Be amenable to some periodic test to detect a device failure indicating a safe reactor condition.
6. Provide for adjustment of parameter limit setpoints.

C. DESIGN CHOICES

The comparator module [Fig. 9] shows the result of several comparisons of techniques. One comparison was among techniques for presenting the parameter limit. Three techniques were considered. The first technique was to enter the parameter into a ROM that had an output of "0" or "1" depending on whether the parameter limit had been exceeded. The second was to store the parameter limit in a core memory and compare it with the parameter measured. The third was

to enter the parameter limit in a local thumbwheel register and have it continuously available to the comparator. This last alternative was chosen as the most practical because the limit was easily changed, it complied with channel separation, and required no data transfers from a common core memory.

Another choice concerned at what point to combine the signal from the four detectors; i.e., the choice of using one of the following as signals into the scram logic modules:

1. A, B, C, D (INDEPENDENTLY)

2. A·C, A+C, B·D, B+D

Choice 2 simplified the logic in the scram logic module and reduced the number of ICs there, possibly improving module mean-time-to-failure (MTTF); however, the added circuitry in the comparator modules negated that MTTF improvement with respect to the overall channel. A second flaw in choice 2 was the transmission of combined signals to the scram logic modules. An IC failure in the comparator module could interrupt some combination of both signals from a signal channel; therefore choice 2 was rejected.

D. DESCRIPTION OF A COMPARATOR MODULE (COM)

As shown in Figure 9 the complement of the parameter reference from a thumbwheel register is directly compared with the digital parameter signal complement. If the signal is smaller, its complement is larger and a logical "1" is gated to a TTL buffer. If the signal input is interrupted or supply voltage to the comparator is lost, an unsafe

condition (logical "0") is gated. The buffer has the capability of sinking larger light-emitting diode turn-on surge currents than standard TTL devices can. This reduces light turn-on time and increases response speed of the photo-isolator. Light turn-off time does not appear to be a function of a surge current. The buffer output drives two photo-isolators whose light-emitting diodes conduct when a safe condition is indicated. The photo-isolators provide independent, electrically isolated, single-parameter signals to each of the scram logic modules. This is the feature that enables digital IC devices to be used in a monitor module.

E. PROGRAM INPUTS TO THE COMPARATOR MODULE

The study of comparator module failure modes led to the realization that not only must the module conform to the single failure criterion, so must the control inputs from the program module since one program module provides inputs to both channels on a comparator module.

Consideration of some technique of comparing program module parameters to determine which of multiple inputs to use as controls for the comparator module led to the conclusion that comparison between program module parameters at the program module level destroyed electrical independence and that the most fruitful concept was to employ two out of three majority voting logic at the comparator control input level. Using this technique, a single failure of a control module or of a control line to a comparator module would not inhibit

operation. The use of photo-isolated program module outputs to the comparator module necessitates the use of a MOS-TTL buffer as the voting circuit. Since a failure in the three control lines to one section of a comparator module will not feed back to the program modules and inhibit their operation, those lines can be considered to belong to that comparator module section. A common mode failure of the control lines can be considered to be the same as a failure of that section of the comparator module.

F. DESCRIPTION OF A SCRAM LOGIC MODULE (SLM)

The Scram Logic Module shown in Figure 10 combines isolated logic signals to give the function: SCRAM = ABC + ABD + BCD + ACD. Catastrophic failure of one SLM cannot be propagated to the other modules of the digital monitor. Diode isolation prevents propagation within the SLM of a short between two inputs of the AND-OR-NOT gate; thus enhancing the fault tree analysis and minimizing the loss of function. A catastrophic failure to the entire module may cause loss of that scram channel. If one signal input channel fails in a no-scram condition, all other channels must operate; therefore, some periodic test for failure in a no-scram condition is required.

G. FAULT TREE OF DIGITAL MONITOR MODULE

Figure 11a is the fault tree of the digital monitor module from final output to the driver inputs to the photo-isolator stages on the COM. Figure 11b is the fault tree for the COM prior to the photo-isolator inputs.

1. Power Supply Failure

Power supply failures were not accounted for in this analysis because a voltage loss to either the COM or SLM would insert a signal tending to cause reactor shut down. The effects of a catastrophically high voltage were uncertain; however, one event that would occur is photo-isolator light-emitting diode burn-out. The cessation of emission would transmit a signal tending to cause reactor shut down also.

2. Wiring Faults

The term "wiring fault" as used in the diagram refers to the worst-case scram-inhibiting casualty to the particular connecting wires or printed circuit; i.e., the only wiring fault applicable to the output wiring of the SLM would be a short to Vcc. Opens, grounds, or very high voltage would result in a shut down signal.

3. Compliance with the Single Failure Criterion

Review of the fault tree for the monitor module itself indicated that no single failure within the module could prevent reactor shut down. The minimum number of failures required was two independent ones, one of the output portion of each scram logic module or of each of two comparator circuits. The use of buffers and diode isolation has minimized propagation of the effects of an IC failure. Reference 25, p.4-7 states that the testing program for the Advanced Multi-Function Array Radar (AMFAR) revealed that failure of TTL integrated circuits, such as proposed here, do not seem to propagate. In that case, seven IC chip failures not corrected by design occurred in 11.2 million operating

hours. No failures propagated to other circuits either on the same chip or connected to the failed circuit.

H. TEST REQUIREMENTS FOR THE MONITOR MODULE

In-service test procedures must identify circuit failures and localize their location at least to the module concerned. The following procedures were adequate to locate defective modules:

1. Turning off the voltage to one program module and inserting unsafe conditions into the comparators, one at a time, functionally tests both remaining program modules, the comparator module, and the interconnecting wiring to the scram logic module.

2. Inserting unsafe conditions into two comparators will functionally test the scram logic modules.

While these tests may be automatic or manual, it is considered that the inherent redundancy and high mean-time-to-failure preclude the need for automatic testing.

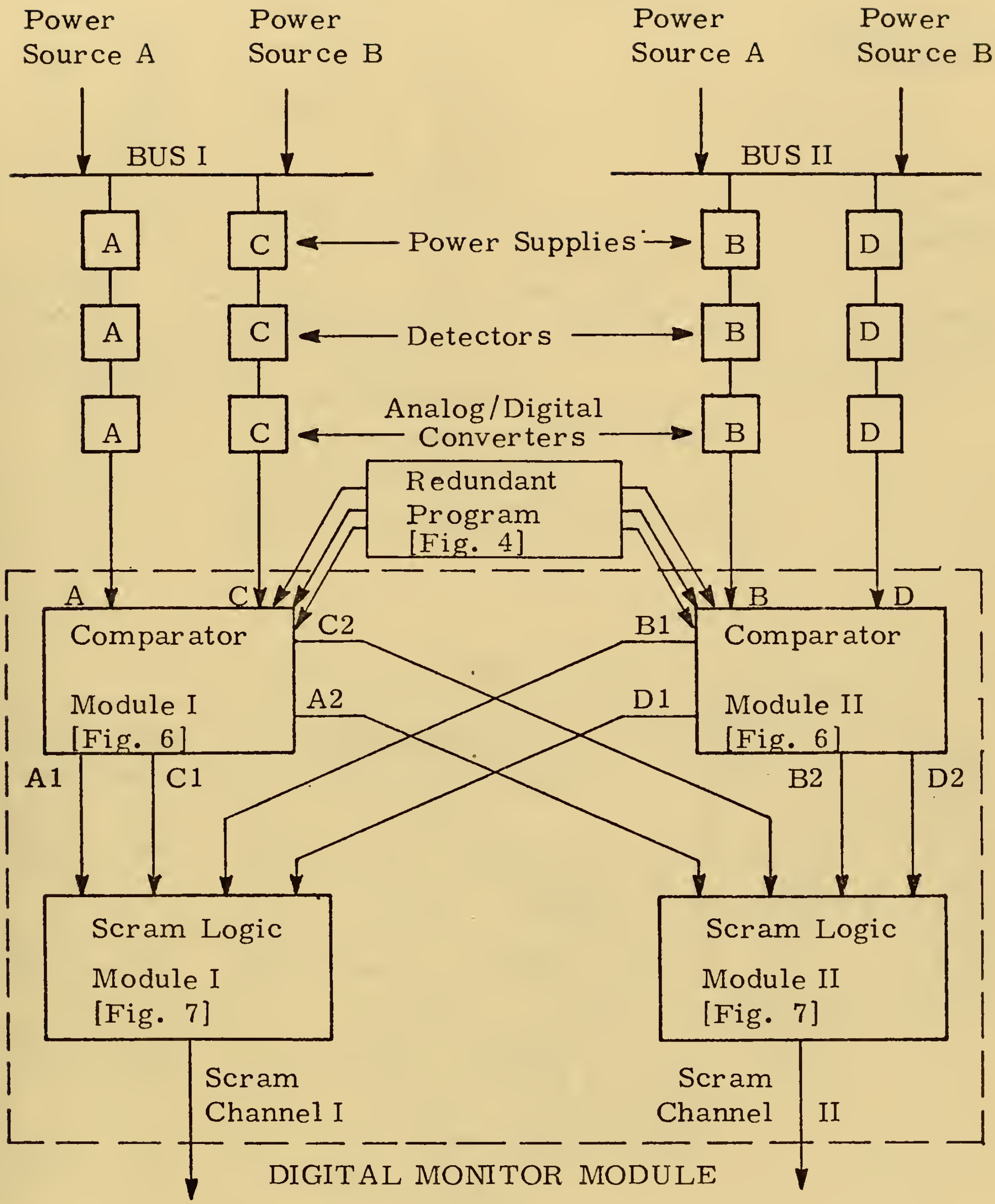
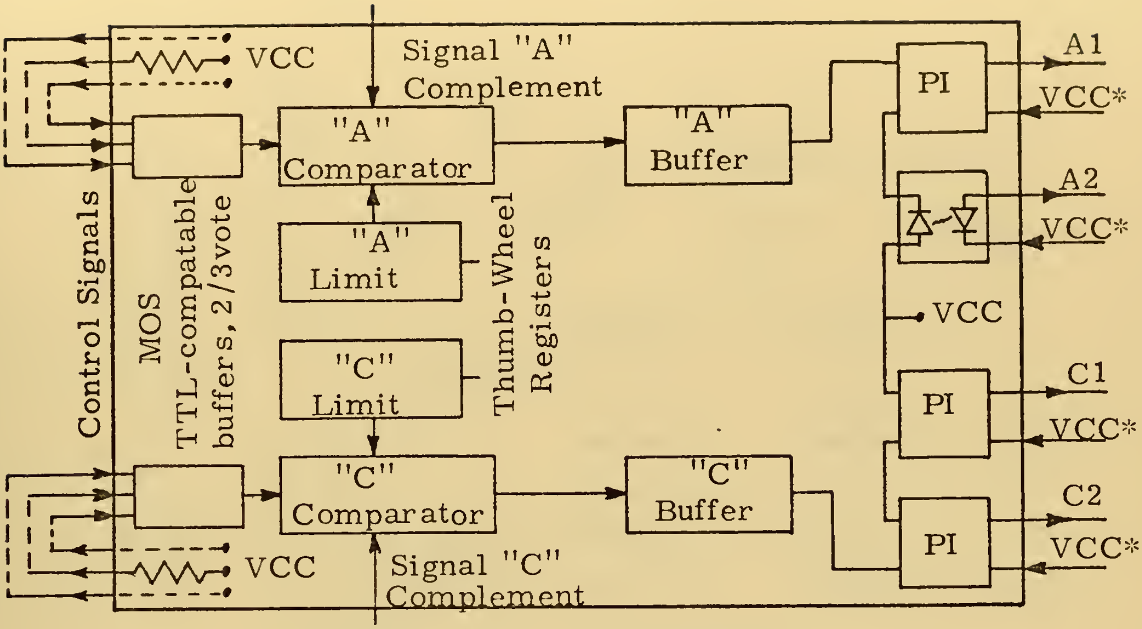


Figure 8. DIGITAL MONITOR CHANNEL



* From scram logic modules
PI - Photo-isolator

Figure 9. COMPARATOR MODULE

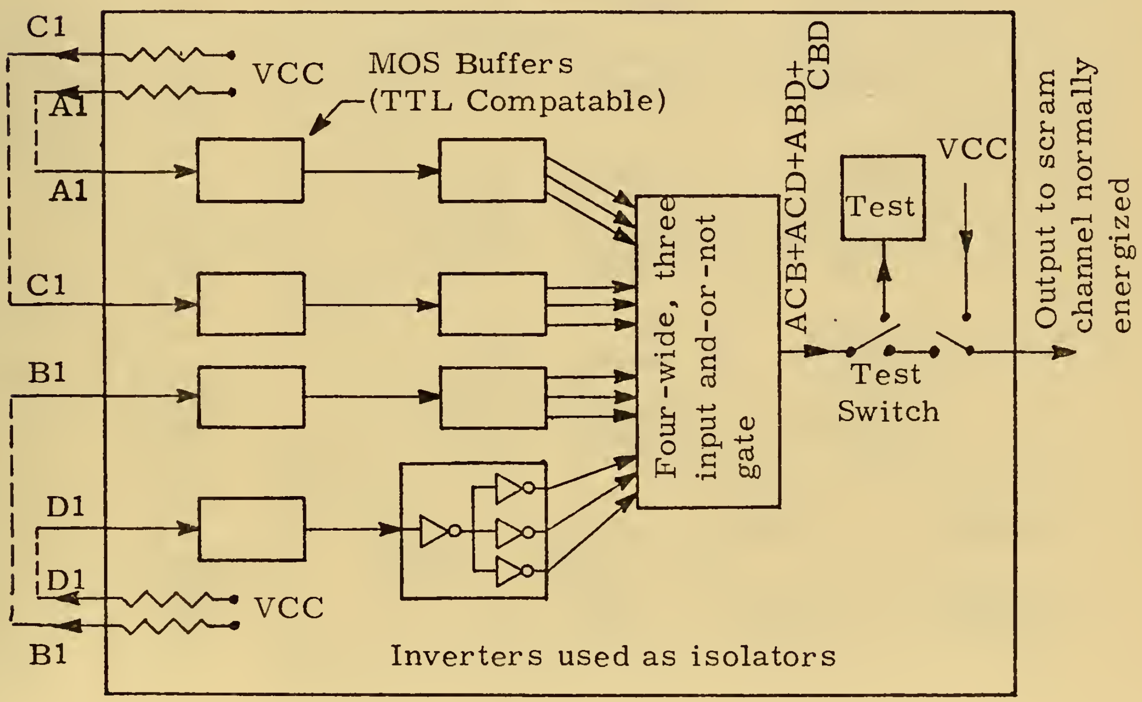
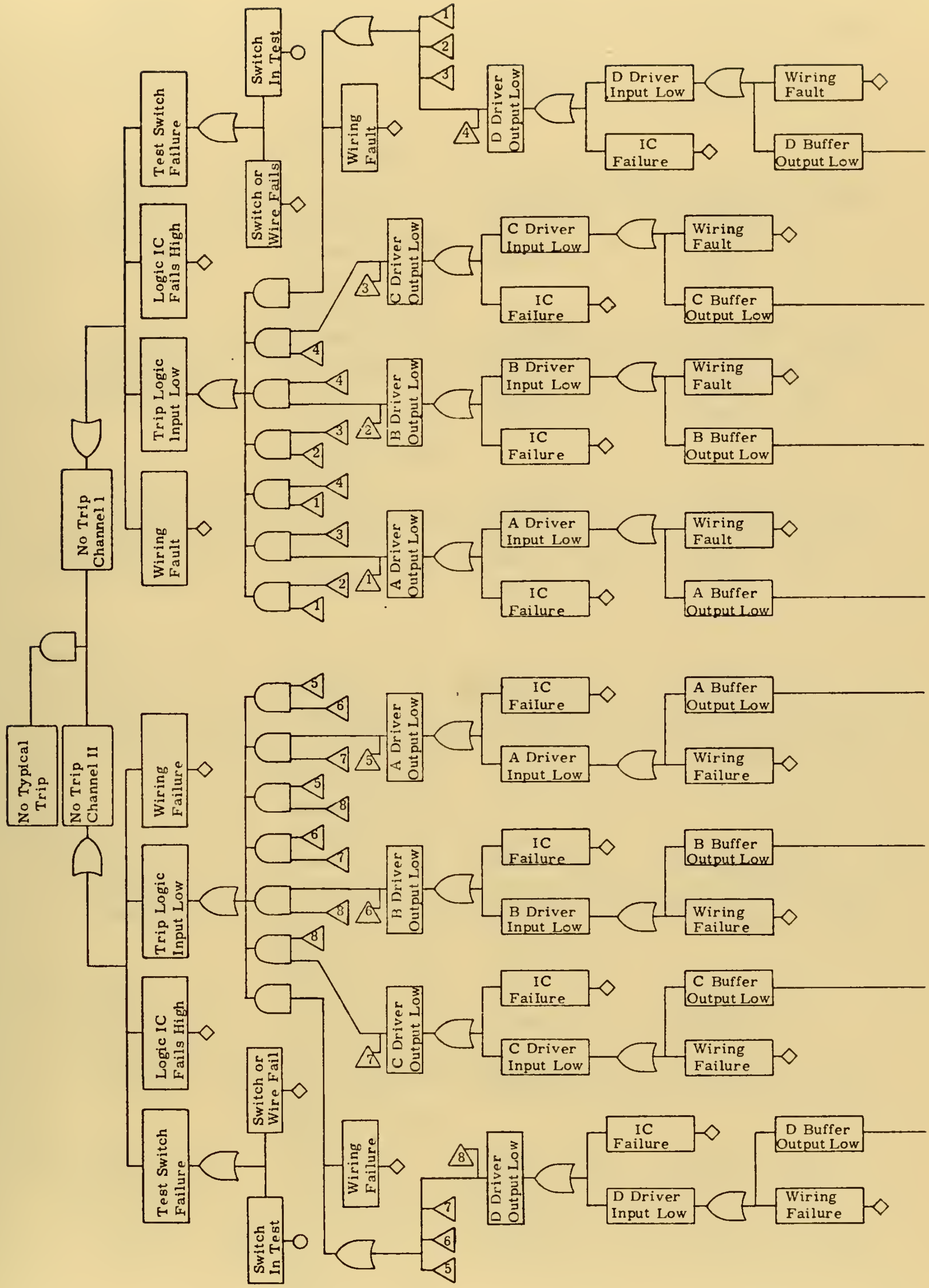


Figure 10. SCRAM LOGIC MODULE


No Typical Trip
No Trip Channel 1
No Trip Channel II
Test Switch Failure
Switch In Test
Switch or Wire Fails
Logic IC Fails High
Trip Logic Input Low
Wiring Fault
Wiring Failure
Switch or Wire Fail
D Driver Output Low
D Driver Input Low
IC Failure
D Buffer Output Low
C Driver Output Low
C Driver Input Low
C Buffer Output Low
B Driver Output Low
B Driver Input Low
B Buffer Output Low
A Driver Output Low
A Driver Input Low
A Buffer Output Low
1
2
3
4
5
6
7
8

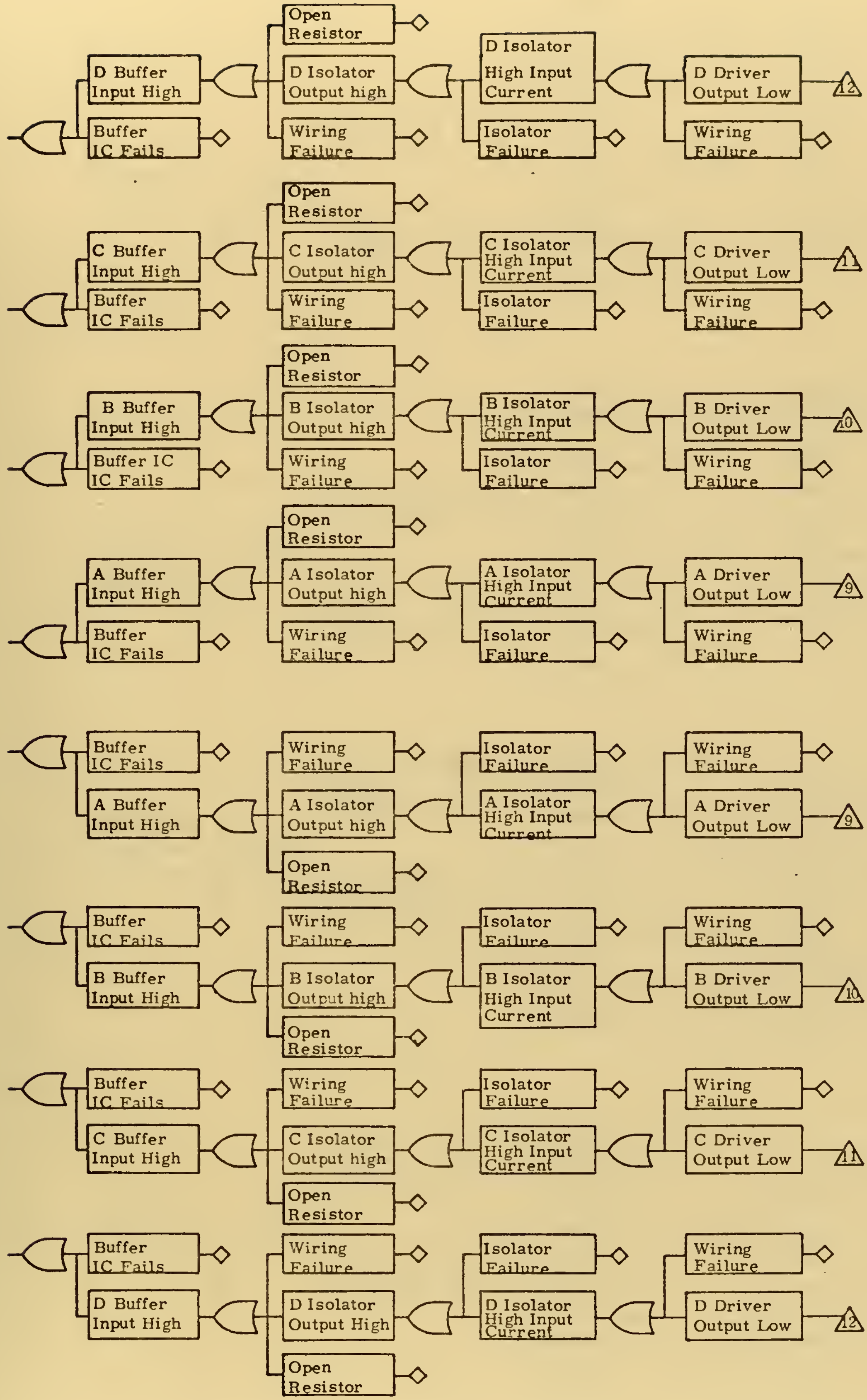


Figure 11a. DIGITAL MONITOR MODULE FAULT TREE

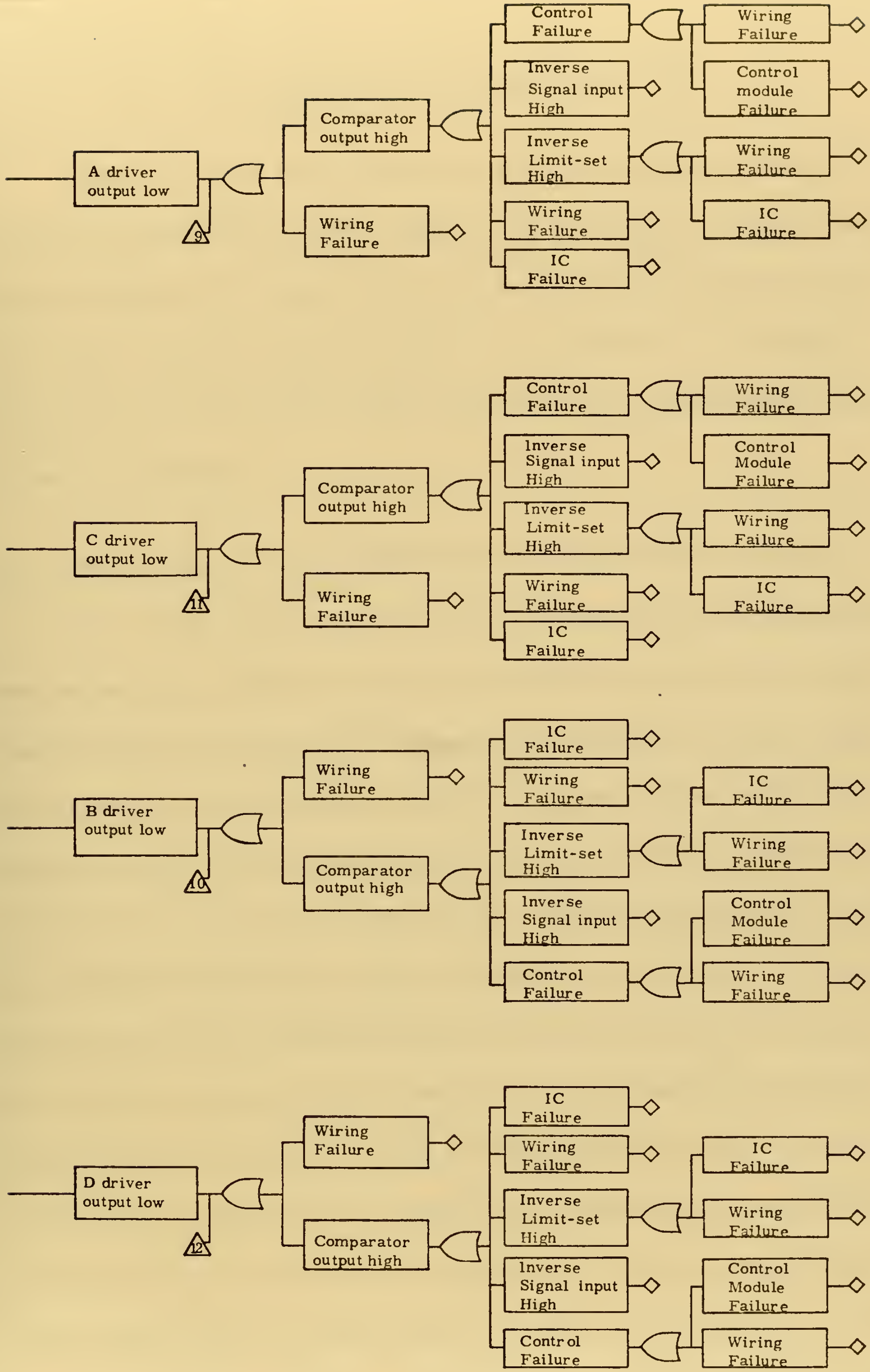


Figure 11b. DIGITAL MONITOR MODULE FAULT TREE

VI. RELIABILITY CONSIDERATIONS

While a reactor safety channel may be considered a sub-set of a general control system, the emphasis of performance and reliability considerations in a reactor safety channel is differentiated from that in a reactor control system because of the differences in method of determination of parameter state and in the desired state after control action is performed.

A. RELIABILITY CONSIDERATIONS IN A CONTROL SYSTEM

In a reactor control system, the desired new state and best resultant action to get there are dependent upon the present reactor state and input demands as well as determination of whether or not the reactor state is safe. One example is the situation where a parameter is sensed by four detectors and one has failed such that an unsafe condition is indicated. The control system must reliably estimate actual reactor state based on those four signals, along with many others, and may well decide that the failed signal will be discarded for control purposes. If the spread in values of the four signals is great enough, the control system may not be able to decide which signals are correct and provision must be made for this possibility. Reference 24 presents the same problem in an aircraft control system. In the aircraft though, when system state is unclear, pilot override is provided and no action or neutral control surface position seems to be considered safer than

some positive action because the operating conditions of the aircraft are too varied to incorporate in the control model. Reliability considerations in a control system are not considered in this paper.

B. RELIABILITY CONSIDERATIONS IN A SAFETY CHANNEL

The action of a nuclear safety channel is to place the reactor in a previously determined safe state if a parameter exceeds a predetermined limit. The limit is calculated allowing for anticipated channel errors.

Primary emphasis in the design of the safety channel is placed on the concept that a single failure will not prevent placing the reactor in a known safe state. The safe state, being pre-determined, usually means shut down and will be so considered here. From a safety standpoint, though perhaps inconvenient, it is acceptable for a single signal or component failure to cause a shut down even though actual reactor conditions are satisfactory. A safe condition in this context is usually inconvenient to the operator. In order to provide assurance that a single failure will not prevent shut down, multiple signal and safety shut down channels are used. In order to provide continuity of operation, voting logic such as one out of two, two out of three or four, or three out of four is used. Design effort is used to cause most signal or device failures to be self-indicating. Periodic tests are used to detect failures that are not self-indicating.

Because the safe reactor state is pre-determined and the safety system is not tasked with the responsibility of determining the exact

state of a parameter, reliability analysis of a safety channel may be reduced to two separate analyses:

(1) probable lifetime of components and connections until one failure occurs (MTBF). This time must exceed the test interval.

(2) fault tree analysis to show that any one failure cannot prevent safety shut down.

For the MTBF of a safety channel, consideration of the series combination of all components and time between single failures, rather than failures that would inhibit shut down, is the most conservative approach. If this arrangement can be shown to be acceptable, then any series/parallel redundant arrangement using the same number of components and connections would be acceptable also.

A MTBF of any failure of 3000 hours or about three months continuous operation of an entire monitor channel was selected as an arbitrary minimum based, not on state-of-the-art, but on presuming a monthly test sequence to assure that proper attention is given to the monitor.

Reliability data for circuits of similar complexity and high quality materials to those incorporated in this design [Ref. 25] gave an in-use estimated microcircuit failure rate of no more than $.192 \times 10^{-6}$ failures/hour. Actual operating results were $7/11.2 \times 10^{+6} = .625 \times 10^{-6}$ failures/hour.

To find the serial failure rate of a module the component failure rates are added. The failure rate per mating of plugs was not included since unplugging modules was not considered to be a normal operating

procedure. The results of these calculations, as given in Table II, indicate that a 3000 hour test interval is reasonable and that, since the program module has no redundant parts, yet has a much higher failure rate than the monitor module, a redundant program module should be provided for an operating installation.

COMPONENT	FAILURES/HR.	REFERENCE	NUMBER PER APPLICATION: SCRAM LOGIC MODULE	COMPARATOR MODULE	PROGRAM MODULE
Integrated Circuit	$.625 \times 10^{-6}$/Hr.	(Ref. 25, p.4-4)	9	12	50
Connector, 16 pin	$.18 \times 10^{-6}$/Hr. .00024/Mating	(Ref. 26, p.7.9-13) (Ref. 26, p.7.9-15)	1	0	0
Connector, 25 pin	$.32 \times 10^{-6}$/Hr. .00070/Mating	(Ref. 26, p.7.9-13) (Ref. 26, p.7.9-15)	0	2	2
Switch, Rotary	$.02 \times 10^{-6}$/Hr.	(Ref. 26, p.7.10-7)	1	0	0
Circuit Board	Negligible	(Ref. 26, p.7.4-1)	1	1	1
Circuit Board Connection	Included in Component	(Ref. 26, p.7.9-1)	-	-	-
Resistor	$.078 \times 10^{-6}$/Hr.	(Ref. 25, p.4-4)	4	6	0
ESTIMATED MODULE			6.4×10^{-6}	8.6×10^{-6}	31.9×10^{-6}

Table II. FAILURE RATE DATA FOR RELIABILITY ESTIMATION

VII. CONCLUSIONS

As a result of this investigation, several conclusions were reached. Some were basic to the initial goal and some became evident as techniques for implementing the circuits were considered.

A. The design indicates that a ROM circuit using isolated outputs--such as the program module--can perform the program functions of a hard-wired sequential controller with an apparent reduction in size and complexity.

B. The meeting of isolation requirements shows that the reactor safety system single failure criterion can be met using TTL ICs and photo-isolators in the safety circuit.

C. External performance monitors tend to reduce independence of redundant circuits, such as the program module, and voting logic downstream of the photo-isolators performs the same task while maintaining redundant module independence.

D. Photo-isolation should be accomplished at signal branch points and should form the upstream terminus of the branch path.

E. Automatic self-test is not always required if enough redundancy is provided.

APPENDIX A

INTRODUCTION TO THE LIQUID METAL FAST BREEDER REACTOR OVERALL PROGRAM PLAN [Ref. 1]

The following remarks are quoted from Ref. 1.

"The Liquid Metal Fast Breeder Reactor (LMFBR) Program has been assigned the highest priority in the Atomic Energy Commission's (AEC) broader program for the development of civilian nuclear power. The primary objective of the civilian power reactor development program in the United States is widespread use of nuclear energy for the production of heat and electricity with full exploitation of the energy available in our resources of uranium and thorium. The AEC's objective also includes fostering the development of a self-sufficient and competitive nuclear industry. The need for a power reactor that can fully and economically exploit the energy reserves contained in uranium and thorium was recognized in the 'Civilian Nuclear Power--A Report to the President--1962' which stated:

> The overall objective of the Commission's nuclear power program should be to foster and support the growing use of nuclear energy, and importantly to guide the program in such directions as to make possible the exploitation of the vast energy resources latent in the fertile materials uranium-238 and thorium.

The breeder is needed because it serves the above objective by: providing the most efficient means of exploiting the energy available in uranium; minimizing the quantity of uranium consumed per unit of

electricity generated; providing potential for low fuel costs; extending ore reserves manyfold by increasing the utilization of uranium recovered from ore; and providing a more effective use for plutonium produced in light-water reactor plants. The 1962 Report to the President includes a detailed discussion of the place to be occupied by the breeder in the overall program.

The 1967 Supplement to the 1962 Report to the President established the following specific objectives: (1) 'The development of improved converter and later breeder reactors to convert the fertile isotopes to fissionable ones, thus making available the full potential of the nuclear fuels;' and (2) 'The early establishment of a self-sufficient and growing nuclear power industry that will assume an increasing share of the development costs.'

In the breeder-reactor concept, excess neutrons produced in the process of generating nuclear power by fission are used to produce more fissionable material than is consumed. The fissionable isotopes U-233, U-235, Pu-239, and Pu-241 all produce more neutrons than are needed to maintain a nuclear chain reaction in power reactors. Reactor designs for large central-station power plants are arranged so that these excess neutrons are absorbed either in U-238, leading to the production of Pu-239, or in thorium, leading to the production of U-233. Of the four fissionable isotopes, only U-233, Pu-239, and Pu-241 produce sufficient neutrons to allow the possibility, in practical power reactors, of producing more fissionable material than is consumed.

The plutonium isotopes produce the most excess neutrons when used as fuel in a fast-neutron reactor, and cycles using U-238 as a fertile material and mixtures of Pu-239 and Pu-241 as a fissile material form the basis of the LMFBR Program. The isotope Pu-241 is formed from Pu-239 through an intermediate isotope, Pu-240, which plays the role of a subsidiary fertile material. The thorium-U-233 cycle is the basis for breeding by using thermal-neutron reactors, but this cycle has received relatively less emphasis in fast breeder reactor development because the potential breeding gain is less than for the plutonium-uranium cycle.

The fast breeders of major interest are divided into three categories: sodium-cooled, gas-cooled, and steam-cooled. The sodium cooled fast breeder has been established as the priority program on the basis of potential economy, probability of successful development interest by reactor manufacturers, and technological experience gained in the United States and abroad. Sodium has a combination of advantageous characteristics:

(1) Good nuclear properties, helpful in attaining high breeding ratios

(2) A high boiling point, allowing high-temperature operation at low pressure--with resultant good plant thermal efficiency without the necessity for thick-walled reactor vessels

(3) Excellent heat transfer, making possible achievement of high specific power and hence low doubling time and fuel cycle costs

(4) A large heat capacity, allowing time for corrective action in the event of a power transient or loss of coolant flow

(5) Low pumping power and relative lack of corrosion in the absence of air and water.

The Program Plan has been developed to lay out the course of action for achieving the objectives of the LMFBR Program. The Plan consists of ten sections, each in a separate volume. Volume 1 presents the Overall Plan. Each of the other nine volumes treats a specific area of the technology in depth by presenting: the objectives to be attained, an evaluation of the state of the art, and the tasks to be carried out to reach the objectives. This Overall Plan describes the scope of each of the nine sections, referred to as Program elements, and the relationships between them."

APPENDIX B

LMFBR PERFORMANCE REQUIREMENTS AND DATA WORD LENGTHS

The following Performance Requirements and resultant binary word lengths required for data transmission were derived from Reference 3, p. 185-294. Binary word lengths include three extra bits for maintenance of accuracy:

1. SENSORS FOR THE DETECTION OF NEUTRONS IN AND NEAR THE CORE

Counter Sensitivity	10^{-5}-10^{-10}CPS/nv
Current Sensitivity	10^{-15}-10^{-19}A/nv
Neutron Flux	10^{11}-10^{16}nv
Range	2 or more decades
BITS for Two Decades Range Arbitrary 1% Accuracy	10

2. SENSORS FOR THE DETECTION OF NEUTRONS OUT OF CORE

Counter Sensitivity	$>$0.7CPS/nv
Current Sensitivity	$> 10^{-14}$A/nv
BITS for Two Decades Range Arbitrary 1% Accuracy	10

3. TEMPERATURE SENSORS FOR GENERAL USE

Range	300-1400 F
Accuracy	$\pm$ 1% on line ($\pm$ 1F test)
Transient Range	to 2000 F
Response Time	unknown
Thermal Shock	max rate 100 F/sec
BITS for 1 F in 2000 F	14

4. TEMPERATURE SENSORS FOR USE IN FUEL

Work is in progress to discover a device that will survive the radiation environment. No specifications are set.

5. SODIUM-FLOW SENSORS FOR USE ON FUEL ASSEMBLIES

Accuracy	$\pm$ 10% of full range
Sensitivity	1% of full range
Time Constant	1/2 second or less
Expected Flow Rates	150 gal/min to 600 gal/min
BITS for 1% Sensitivity	10

6. SODIUM-FLOW SENSORS FOR USE IN PIPES

Accuracy	$\pm$ 5% of actual flow (above 10% flow)
Dynamic Range	10:1 to 100:1
Flow Range	0 to 120,000 gal/min
BITS for 5% Accuracy	8

7. PRESSURE SENSORS FOR USE IN OR NEAR CORE

Range: 0-15 PSI, absolute and gage pressure.

0-20 in through 0-400 in water column, differential pressure.

PURPOSE	ACCURACY	TIME CONSTANT
Safety	± 3.0%	< 0.1 sec
	± 10.0% dynamic	< 0.001 sec
Plant Control	± 0.5%	< 10.0 sec
	± 3.0%	< 0.1 sec
BITS for 0.5% Accuracy		11

8. PRESSURE SENSORS FOR USE ON PIPES OR VESSELS

Same as item 7.

9. PRESSURE SENSORS FOR USE ON FUEL ELEMENTS

Range	0-300 through 0-3000 psi
Drift	< 0.1% full scale per week
Response time	< 2.0 min
BITS for 0.1% Accuracy	13

10. SODIUM LEVEL SENSORS

Range	0-1 ft. to 0-50 ft.
Accuracy	± 1/2 in. to ± several in.
Response time	1 sec to 10 sec
BITS for 1 in/50 ft	13

11. STRAIN SENSORS FOR USE ON PLANT, CORE, AND FUEL COMPONENTS

Microstrain Range	$\pm$ 2000 $\mu\epsilon$
Drift	$<$ 2.0 $\mu\epsilon$/hr.
Gage Factor	$>$ 1.5
Linearity	unknown
BITS for 2000 $\mu\epsilon$	14

$\pm$ 1 $\mu\epsilon$ Arbitrary

APPENDIX C

COMPUTER MODEL DEMONSTRATION OF THE DIGITAL PROGRAM MODULE

THIS MODEL SIMULATES THE PHYSICAL ACTION OF THE PROGRAM MODULE (FIG.1). THE CONTENTS OF THE PROMS ARE SIMULATED BY THE SAME TYPE VECTOR AS THE ACTUAL USE OF THE PROM DEDICATED BIT; I.E., A LOGICAL USE IS REPRESENTED BY A LOGICAL VECTOR. IN THE MODEL, THE SYNC INPUT IS ASSUMED 'ON' AND ADDRESSES OF PROM WORDS START AT '1' VICE '0' BECAUSE ARRAYS CANNOT HAVE A '0' ADDRESS .

1. DEFINITION OF TERMS USED

PAR = DECIMAL STATE OF PROGRAM ADDRESS REGISTER. PHYSICALLY, IT IS A MODULO 256 BINARY COUNTER. PAR ADDRESSES ROM-RP.

RPA = A DECIMAL VECTOR REPRESENTING BITS 0-2 OF RP WORDS AND CONTAINING THE NUMBER OF TIMES THE SUBROUTINE IS TO BE REPEATED.

RPB = A LOGICAL VECTOR REPRESENTING BIT 3 OF ROM-RP WORDS. '0' = START OF SUBROUTINE COINCIDES WITH A SYNC PULSE.

RPC = A DECIMAL(0-1021) VECTOR REPRESENTING BITS 4-11 OF ROM-RP WORDS AND TWO '0' LEAST SIGNIFICANT BITS. RPC IS THE START ADDRESS OF THE NEXT SUBROUTINE AND IS PROVIDED AS THE PARALLEL INPUT INTO THE SUBROUTINE ADDRESS REGISTER - SAR.

SAR = DECIMAL STATE OF SUBROUTINE ADDRESS REGISTER. PHYSICALLY, IT IS A MODULO 1024 BINARY COUNTER. SAR ADDRESSES ROM-RS.

RSA = A LOGICAL VECTOR REPRESENTING BIT 0 OF ROM-RS WORDS. RSA = 1 ONLY AT THE END OF A SUBROUTINE.

RSB = A LOGICAL VECTOR REPRESENTING BIT 1 OF ROM-RS WORDS RSB = 1 ONLY AT THE START OF A SUBROUTINE. RSB = 1 CLOCKS PAR AND PCR.

RSC = A DECIMAL VECTOR REPRESENTING BITS 2-(N+2) OF ROM-RS. THE MODEL CONTAINS THE ADDRESS OF THAT WORD. PHYSICALLY, N INDEPENDENT LOGICAL OPERATORS WOULD EXIST IN RSC.

CET = COUNT ENABLE FOR SAR.

PE = PARALLEL ENABLE FOR SAR (ACTIVE LOW). PARALLEL ENTRY =((.NOT.PE).AND.CET).

PCR = PROGRAM COUNT REGISTER - CONTROLS PCRB.

PCRB= COUNT ENABLE FOR PAR.

CLOCK=10 MHZ DIGITAL CLOCK INTO SAR.

SYNC= SYNC INPUT FOR THE START OF SUBROUTINES DESIGNATED BY A '0' ON RPB BUS.

2. FLOW DIAGRAM OF THE COMPUTER MODEL

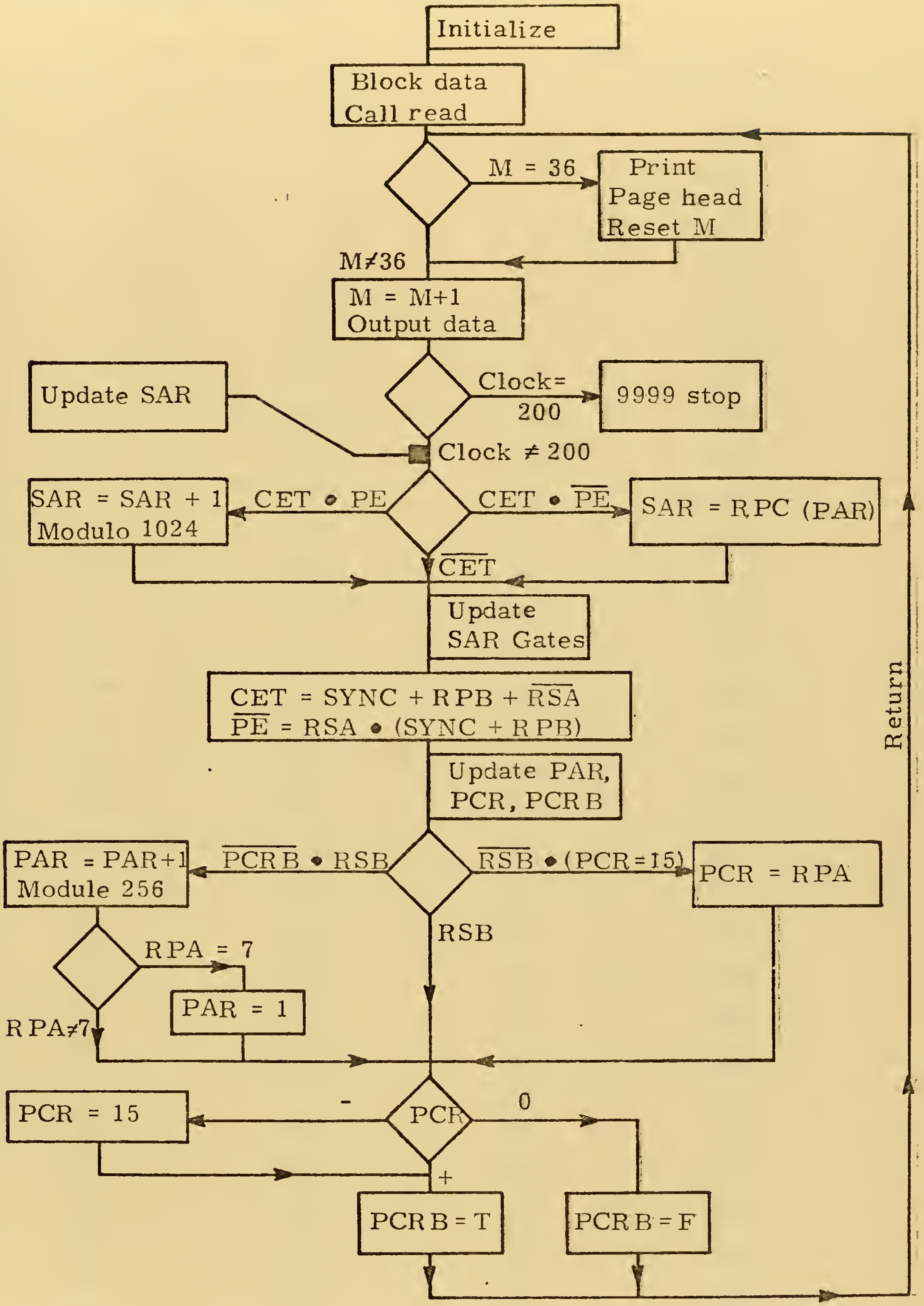


Figure 12. FLOW CHART FOR COMPUTER SIMULATION OF PROGRAM MODULE

3. CONTENTS OF PROGRAM PROM, ADDRESS I

I	RPA	RPB	RPC	I	RPA	RPB	RPC
1	1	T	17	33	7	T	1021
2	1	F	5	34	7	T	1021
3	0	T	21	35	7	T	1021
4	0	T	5	36	7	T	1021
5	1	F	9	37	7	T	1021
6	7	T	1021	38	7	T	1021
7	7	T	1021	39	7	T	1021
8	7	T	1021	40	7	T	1021
9	7	T	1021	41	7	T	1021
10	7	T	1021	42	7	T	1021
11	7	T	1021	43	7	T	1021
12	7	T	1021	44	7	T	1021
13	7	T	1021	45	7	T	1021
14	7	T	1021	46	7	T	1021
15	7	T	1021	47	7	T	1021
16	7	T	1021	48	7	T	1021
17	7	T	1021	49	7	T	1021
18	7	T	1021	50	7	T	1021
19	7	T	1021	51	7	T	1021
20	7	T	1021	52	7	T	1021
21	7	T	1021	53	7	T	1021
22	7	T	1021	54	7	T	1021
23	7	T	1021	55	7	T	1021
24	7	T	1021	56	7	T	1021
25	7	T	1021	57	7	T	1021
26	7	T	1021	58	7	T	1021
27	7	T	1021	59	7	T	1021
28	7	T	1021	60	7	T	1021
29	7	T	1021	61	7	T	1021
30	7	T	1021	62	7	T	1021
31	7	T	1021	63	7	T	1021
32	7	T	1021	64	7	T	1021

4. CONTENTS OF SUBROUTINE PROM, ADDRESS I

I	RSA	RSB	RSC	I	RSA	RSB	RSC
1	T	F	1	33	T	T	33
2	F	F	2	34	T	T	34
3	T	F	3	35	T	T	35
4	F	F	4	36	T	T	36
5	F	T	5	37	T	T	37
6	F	F	6	38	T	T	38
7	F	F	7	39	T	T	39
8	T	F	8	40	T	T	40
9	F	T	9	41	T	T	41
10	F	F	10	42	T	T	42
11	T	F	11	43	T	T	43
12	F	F	12	44	T	T	44
13	F	T	13	45	T	T	45
14	F	F	14	46	T	T	46
15	F	F	15	47	T	T	47
16	T	F	16	48	T	T	48
17	F	T	17	49	T	T	49
18	F	F	18	50	T	T	50
19	T	F	19	51	T	T	51
20	F	F	20	52	T	T	52
21	F	T	21	53	T	T	53
22	F	F	22	54	T	T	54
23	F	F	23	55	T	T	55
24	T	F	24	56	T	T	56
25	F	T	25	57	T	T	57
26	F	F	26	58	T	T	58
27	T	F	27	59	T	T	59
28	F	F	28	60	T	T	60
29	F	T	29	61	T	T	61
30	F	F	30	62	T	T	62
31	F	F	31	63	T	T	63
32	T	F	32	64	T	T	64

5. RESULTANT ACTION OF PROGRAM MODULE

CLOCK	SAR	CET	PE	RSA	RSB	RSC	PCR	PCRB	PAR	RPA	RPB	RPC
0	1	T	F	T	F	1	1	T	1	1	T	17
1	17	T	T	F	T	17	0	F	1	1	T	17
2	18	T	T	F	F	18	0	F	1	1	T	17
3	19	T	F	T	F	19	0	F	1	1	T	17
4	17	T	T	F	T	17	15	T	2	1	F	5
5	18	T	T	F	F	18	1	T	2	1	F	5
6	19	T	F	T	F	19	1	T	2	1	F	5
		SYNC	REQUIRED					SYNC	REQUIRED			
7	5	T	T	F	T	5	0	F	2	1	F	5
8	6	T	T	F	F	6	0	F	2	1	F	5
9	7	T	T	F	F	7	0	F	2	1	F	5
10	8	T	F	T	F	8	0	F	2	1	F	5
		SYNC	REQUIRED					SYNC	REQUIRED			
11	5	T	T	F	T	5	15	T	3	0	T	21
12	6	T	T	F	F	6	0	F	3	0	T	21
13	7	T	T	F	F	7	0	F	3	0	T	21
14	8	T	F	T	F	8	0	F	3	0	T	21
15	21	T	T	F	T	21	15	T	4	0	T	5
16	22	T	T	F	F	22	0	F	4	0	T	5
17	23	T	T	F	F	23	0	F	4	0	T	5
18	24	T	F	T	F	24	0	F	4	0	T	5
19	5	T	T	F	T	5	15	T	5	1	F	9
20	6	T	T	F	F	6	1	T	5	1	F	9
21	7	T	T	F	F	7	1	T	5	1	F	9
22	8	T	F	T	F	8	1	T	5	1	F	9
		SYNC	REQUIRED					SYNC	REQUIRED			
23	9	T	T	F	T	9	0	F	5	1	F	9
24	10	T	T	F	F	10	0	F	5	1	F	9
25	11	T	F	T	F	11	0	F	5	1	F	9
		SYNC	REQUIRED					SYNC	REQUIRED			
26	9	T	T	F	T	9	15	T	1	1	T	17
27	10	T	T	F	F	10	1	T	1	1	T	17
28	11	T	F	T	F	11	1	T	1	1	T	17
29	17	T	T	F	T	17	0	F	1	1	T	17
30	18	T	T	F	F	18	0	F	1	1	T	17
31	19	T	F	T	F	19	0	F	1	1	T	17
32	17	T	T	F	T	17	15	T	2	1	F	5
33	18	T	T	F	F	18	1	T	2	1	F	5
34	19	T	F	T	F	19	1	T	2	1	F	5
		SYNC	REQUIRED					SYNC	REQUIRED			
35	5	T	T	F	T	5	0	F	2	1	F	5

6. MAIN SIMULATION PROGRAM

```
C     INITIALIZE VARIABLES

      COMMON/BLK1/RPA,RPB,RPC/BLK2/RSA,RSB,RSC
     */BLK3/PAR,SAR,PCR,CLOCK,M,CET,PE,SYNC,PCRB
      INTEGER PAR,SAR,RPA(256),RPC(256),RSC(1024),CLOCK,PCR
      LOGICAL PCRB,RSB(1024),RPB(256), PE,CET,SYNC,RSA(1024)

C     READ IN INITIAL CONDITIONS (COMPLETE RESET)
C     READ IN CONTENTS OF ARRAYS SIMULATING ROMS
C     PRINT OUT ARRAYS SIMULATING ROMS

      CALL READ

C     STATEMENT 5 PROVIDES A RETURN FOR ITERATION
C     PRINT PAGE HEADINGS IF NECESSARY
C     INCREMENT LINE COUNTER (M)

    5 IF(M.LT.36) GO TO 9
      WRITE(6,8)
    8 FORMAT('1',//// ,T16,'5.  RESULTANT ACTION OF PROGRAM'
     *,' MODULE',//,T16,'CLOCK',T22,'SAR',T26,'CET',T31,'PE'
     *,T34,'RSA',T38,'RSB',T43,'RSC',T47,'PCR',T52,'PCRB',
     *T57,'PAR',T63,'RPA',T67,'RPB',T72,'RPC',/)
      M=0
    9 M=M+1

C     PRINT CURRENT STATE AT END OF CLOCK PULSE
C     DETERMINE NEED FOR SYNC AND START NEW CLOCK PULSE
C     IF ITERATIONS ARE COMPLETED, GO TO 'STOP'

      WRITE(6,13)CLOCK,SAR,CET,PE,RSA(SAR),RSB(SAR),
     *RSC(SAR),PCR,PCRB,PAR,RPA(PAR),RPB(PAR),RPC(PAR)
   13 FORMAT(13X,2I5,4L4,I6,I4,L5,I5,I5,L4,I6)
      IF(RSA(SAR).AND..NOT.RPB(PAR))WRITE(6,16)
   16 FORMAT(24X,2(13HSYNC REQUIRED,15X))
      IF(CLOCK.EQ.200)GO TO 9999
      CLOCK=CLOCK+1

C     UPDATE SAR

      IF(.NOT.CET) GO TO 21
      IF(CET.AND..NOT.PE) SAR=RPC(PAR)
      IF(CET.AND.PE) SAR = SAR+1
   21 IF(SAR-1025) 23,22,9000
   22 SAR = 1
   23 CONTINUE

C     UPDATE SAR ENABLE GATES: PE-CET
C     USING CURRENT CLOCK RS OUTPUT AND LAST CLOCK RP OUTPUT

      CET=SYNC.OR.RPB(PAR).OR..NOT.RSA(SAR)
      PE = .NOT.(RSA(SAR).AND.(SYNC.OR.RPB(PAR)))

C     UPDATE PAR, RESET PAR IF RPA(PAR)=7

      IF(PCRB.OR..NOT.RSB(SAR)) GO TO 32
      PAR=PAR+1
      IF(PAR-257) 32,31,9001
   31 PAR = 1
   32 IF(RPA(PAR).EQ.7) PAR=1
```

```
C      UPDATE PCR AND PCRB

       IF(.NOT.RSB(SAR)) GO TO 44
       PCR = PCR - 1
    40 IF(PCR) 41,42,43
    41 PCR = 15
       GO TO 43
    42 PCRB=.FALSE.
       GO TO 5
    43 PCRB=.TRUE.
       GO TO 5
    44 IF (PCR-15) 40,45,9002
    45 PCR = RPA(PAR)
       GO TO 40

C      ERROR MESSAGES

  9000 WRITE(6,9500)
  9500 FORMAT(10X,35HSUBROUTINE ADDRESS REGISTER OVERRUN)
       GO TO 9999
  9001 WRITE(6,9501)
  9501 FORMAT(10X,32HPROGRAM ADDRESS REGISTER OVERRUN)
       GO TO 9999
  9002 WRITE(6,9502)
  9502 FORMAT(10X,32HPROGRAM CONTROL REGISTER OVERRUN)

  9999 STOP
       END
```

7. BLOCK DATA INPUT

```
       BLOCK DATA
       COMMON/BLK1/RPA,RPB,RPC/BLK2/RSA,RSB,RSC
      */BLK3/PAR,SAR,PCR,CLOCK,M,CET,PE,SYNC,PCRB
       INTEGER PAR,SAR,RPA(256),RPC(256),RSC(1024),CLOCK,PCR
       LOGICAL PCRB,RSB(1024),RPB(256), PE,CET,SYNC,RSA(1024)
       DATA RPA/256*7/,RPB/256*.TRUE./,RPC/256*1021/,RSA/
      #1024*.TRUE./,RSB/1024*.TRUE./,PCRB/.TRUE. /
       DATA PAR/  1/, SAR/    1/,PCR/ 1/,CLOCK/0/,M/36/
       DATA CET/.TRUE. /,PE/.FALSE./,SYNC/.TRUE./
       END
```

8. SUBROUTINE 'READ'

```
      SUBROUTINE READ
C     READ IN INITIAL CONDITIONS
C     READ IN CONTENTS OF ARRAYS SIMULATING ROMS
C     PRINT OUT ARRAYS SIMULATING ROMS

      COMMON/BLK1/RPA,RPB,RPC/BLK2/RSA,RSB,RSC
     */BLK3/PAR,SAR,PCR,CLOCK,M,CET,PE,SYNC,PCRB
      INTEGER PAR,SAR,RPA(256),RPC(256),RSC(1024),CLOCK,PCR
      LOGICAL PCRB,RSB(1024),RPB(256), PE,CET,SYNC,RSA(1024)

C     READ IN ARRAYS FOR ROMS-RS AND RP

      READ(5,108)(RPA(I),RPB(I),RPC(I),I=1,5)
  108 FORMAT(8(I2,L2,I6))
      READ(5,109)(RSA(I),RSB(I),RSC(I),I=1,32)
  109 FORMAT(8(2L2,I6))
      DO 110 I=1,1024
  110 RSC(I)=I

C     PRINT OUT ARRAYS FOR ROM-RP

      N=0
      L=0
      DO 150 I=1,128
      IF(N)143,143,145
  143 WRITE(6,144)
  144 FORMAT('1',//// ,15X,'3.  CONTENTS OF PROGRAM PROM'',
     *', ADDRESS I',
     *//,24X,2('I',3X,'RPA',1X,'RPB',2X,'RPC',11X),/)
  145 L=L+1
      NN=L+32
      N=N+1
      WRITE(6,146) L,RPA(L),RPB(L),RPC(L),
     *NN,RPA(NN),RPB(NN),RPC(NN)
  146 FORMAT( T23,2(2I4,L4,I6,9X),/)
      IF(N.EQ.32)L=L+32
      IF(N.EQ.32)N=0
  150 CONTINUE

C     PRINT OUT ARRAYS FOR ROM-RS

      N=0
      L=0
      DO 160 I=1,512
      IF(N)153,153,155
  153 WRITE(6,154)
  154 FORMAT('1',//// ,15X,'4.  CONTENTS OF SUBROUTINE'',
     *' PROM, ADDRESS I',/
     *//,24X,2('I',3X,'RSA',1X,'RSB',2X,'RSC',11X),/)
  155 L=L+1
      NN=L+32
      N=N+1
      WRITE(6,156)L,RSA(L),RSB(L),RSC(L),
     *NN,RSA(NN),RSB(NN),RSC(NN)
  156 FORMAT(T23,2(I4,2L4,I6,9X),/)
      IF(N.EQ.32)L=L+32
      IF(N.EQ.32)N=0
  160 CONTINUE

      END
```

BIBLIOGRAPHY

1. LMFBR Program Office, Argonne National Laboratory Report WASH 1101, Liquid Metal Fast Breeder Reactor Program Plan, Volume I, Overall Plan, August 1968.

2. LMFBR Program Office, Argonne National Laboratory Report WASH 1103, Liquid Metal Fast Breeder Reactor Program Plan, Volume III, Components, August 1968.

3. LMFBR Program Office, Argonne National Laboratory Report WASH 1104, Liquid Metal Fast Breeder Reactor Program Plan, Volume IV, Instrumentation and Control, August 1968.

4. LMFBR Program Office, Argonne National Laboratory Report WASH 1106, Liquid Metal Fast Breeder Reactor Program Plan, Volume VI, Core Design, August 1968.

5. LMFBR Program Office, Argonne National Laboratory Report WASH 1110, Liquid Metal Fast Breeder Reactor Program Plan, Volume X, Safety, August 1968.

6. Feit, Ronald, "Liquid Metal Fast Breeder Reactor Instrumentation," IEEE Transactions on Industrial Electronics and Control Instrumentation, v. IECI-16, p. 81-94, July 1969.

7. Billeter, T.R. and Brown, D.P., "High Temperature Measurement Instruments for Advanced Reactors," American Nuclear Society Transactions, v. ANS 13 SUP. 14, p. 15-16, 1970.

8. Upton, J. W., Brown, D. P. and Spear, W. C., "In-Core, Self Powered Fast Neutron Flux Monitors," American Nuclear Society Transactions, v. ANS 13 SUP. 14, p. 14, 1970.

9. Porter, N.S., Hoitink, N.C. and Jackson, C.N. Jr., "In-Core Detector Cables: Signals or Noise," American Nuclear Society Transactions, v. ANS 13 SUP. 14, p. 14-15, 1970.

10. Babcock and Wilcox Report BAW-1316, LMFBR Follow-on Study, Task I Report, Concept III System, v. 4, July 1967.

11. Allen, Russell E., "Stand by Power Supplies for Nuclear Generating Stations," IEEE Transactions on Nuclear Science, v. NS-17, no. 1, p. 608-615, February 1970.

12. Nathan, A., "Nuclear Plant Protective Systems," Power Engineering, p. 64-67, March 1968.

13. Institute of Electrical and Electronics Engineers Standard No. 308, IEEE Criteria for Class IE Electric Systems for Nuclear Power Generating Stations, September 11, 1969.

14. Institute of Electrical and Electronics Engineers Standard No. 279, Proposed IEEE Criteria for Nuclear Power Plant Protection Systems, August 1968.

15. Subcommittee 5, Reliability, IEEE/JCNPS, General Principles for Reliability Analysis of Nuclear Power Generating Station Protection Systems, DRAFT 3, (not approved by IEEE), August 1971.

16. Lipinski, Walter C. and Vacroux, Andre G., "Optimal Digital Computer Control of Nuclear Reactors," IEEE Transactions on Nuclear Science, v. NS-17, No. 1, p. 510-516, February 1970.

17. Loupa, J.A. and Anderton, R.D., "Direct Digital Control of a Nuclear Power Reactor," IEEE Transactions on Nuclear Science, v. NS-17, No. 1, p. 586-593, February 1970.

18. Lunde, J.E., "Computer Control Developments at the OECD Halden Reactor Project," American Nuclear Society Transactions, v. ANS 13, No. 2, p. 463, November 1970.

19. "On-Line Computer for Nuclear Reactors," Nuclear Engineering International, p. 950-952, November 1968.

20. Powers, D.V. and Ward, T.J., "Digital Control of Nuclear Power Reactors," American Nuclear Society Transactions, v. ANS 13, No. 1, p. 239-240, June-July 1970.

21. Lawrence, B.R. and Epler, E.P., "Further Use of On-Line Digital Computers in the Operation of Power Reactors," Nuclear Safety, v. 7, No. 4, p. 456-458, Summer 1966.

22. Davis, D. and Darker, H.A., "A Hybrid Computer Study of Direct Digital Control of a Nuclear Power Station," Analog and Hybrid Computation Applied to Nuclear Energy, p. 280-300, Brussels, Presses Academiques Europeennes, 1969.

23. Spurgin, A.J., "Some Aspects of the Process Control and Protection Systems of a Westinghouse PWR," IEEE Transactions on Nuclear Science, v. NS-17, No. 1, p. 608-615, February 1970.

24. Sutherland, J.P., "Fly-By-Wire Flight Control Systems," Advisory Group for Aerospace Research & Development Conference Proceedings, No. 58, January 1970.

25. Bird Engineering-Research Associates, Inc., Final Report, Advanced Multi-Function Array Radar (AMFAR), Reliability-Maintainability Assessment, October 15, 1971.

26. Department of Defense MIL-HDBK-217A, Reliability Stress and Failure Rate Data for Electronic Equipment, December 1, 1965.

INITIAL DISTRIBUTION LIST

		No. Copies
1.	Defense Documentation Center Cameron Station Alexandria, Virginia 22314	2
2.	Library, Code 0212 Naval Postgraduate School Monterey, California 93940	2
3.	Professor Mitchell L. Cotton, Code 52Cc Department of Electrical Engineering Naval Postgraduate School Monterey, California 93940	1
4.	LCDR Stephen A. Elrod, USN 1149 Powell Court S.E. Atlanta, Georgia 30316	1
5.	Professor S. R. Parker Department of Electrical Engineering Naval Postgraduate School Monterey, California 93940	1

DOCUMENT CONTROL DATA - R & D

(Security classification of title, body of abstract and indexing annotation must be entered when the overall report is classified)

1. ORIGINATING ACTIVITY *(Corporate author)* Naval Postgraduate School Monterey, California 93940	2a. REPORT SECURITY CLASSIFICATION Unclassified
	2b. GROUP

3. REPORT TITLE

Application of Digital Techniques to a Nuclear Reactor Safety Monitor for the Liquid Metal Fast Breeder Reactor

4. DESCRIPTIVE NOTES *(Type of report and, inclusive dates)*

Master's Thesis; (March 1972)

5. AUTHOR(S) *(First name, middle initial, last name)*

Stephen Anthony Elrod

6. REPORT DATE	7a. TOTAL NO. OF PAGES	7b. NO. OF REFS
March 1972	72	26

8a. CONTRACT OR GRANT NO.	9a. ORIGINATOR'S REPORT NUMBER(S)
b. PROJECT NO.	
c.	9b. OTHER REPORT NO(S) *(Any other numbers that may be assigned this report)*
d.	

10. DISTRIBUTION STATEMENT

Approved for public release; distribution unlimited.

11. SUPPLEMENTARY NOTES	12. SPONSORING MILITARY ACTIVITY
	Naval Postgraduate School Monterey, California 93940

13. ABSTRACT

This paper demonstrates a nuclear reactor safety monitor incorporating hard-wired, redundant, digital program modules that control independent, redundant, digital monitor modules. One monitor module is used for each parameter significant to reactor safety. The characteristics of a proposed LIQUID METAL FAST BREEDER REACTOR are used as the reference performance criteria. The established criterion that a single failure must not prevent reactor shut down is used as the failure mode criterion. Within the program module, a programmable read-only memory (PROM) is used for sequence control of another PROM containing variable length subroutines. The subroutine PROM outputs are used as photo-isolated logic outputs for sequence control of the various monitor modules. The program module action is modelled on a digital computer. A four-input digital monitor module is developed. This module provides a shut down signal if three of the inputs exceed the parameter limit.

KEY WORDS	LINK A		LINK B		LINK C	
	ROLE	WT	ROLE	WT	ROLE	WT
Liquid Metal Cooled Reactor						
Safety Devices						
Nuclear Reactor Safety						
Digital Techniques						

Thesis 135265
E427 Elrod
c.1
Application of digital techniques to a nuclear reactor safety monitor for the liquid metal fast breeder reactor.